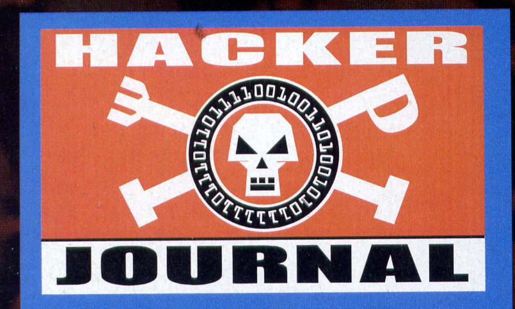


HACKER JOURNAL
www.hacker-journal.com
LINUX
Alejando
a los intrusos
2€
SIN PUBLICIDAD
SÓLO INFORMACIÓN
Y ARTÍCULOS
El cifrado
de doble clave
Los fundamentos
de la criptografía
moderna
EL SÍNDROME DE CHINA
China e Internet,
una relación peligrosa
MISTERIO 23
La historia
del hacker alemán
Karl Koch
LOS PUERTOS
Y SERVICIOS
MENOS
CONOCIDOS
A veces vuelven
Cómo borrar de
verdad archivos
reservados
N. 5
4ever
00005
8 414090 031417
PRÁCTICA
SEGURIDAD
VIRUS
LINKS



Año 2 - N. 5
Marzo-Abril 2004

Director Responsable:
Luca Sprea

Los chicos de la redacción europea:
Federico Cociancich, Amadeu Brugués, Infoambiente, Ana Esteban, Gualtiero Tronconi, Eduardo Bracaglia

Colaboradores: Bismark, Fabio Benedetti, Guillermo Cancelli, Gaia, Nicolás A., Lele, Roberto "decOder" Enea, >>>----Robin---->, Lidia,3dO, Mònica Batalla, Anna Riera

Maquetación: Estudi Digital, S.L.

Diseño gráfico: Dopla Graphic S.r.l.
info@dopla.com

Redacción
4ever S.r.l.
Via Torino, 51
20063 Cernusco S/N (MI)
Fax +39/02.92.43.22.35

Printed in Italy

Distribución
Coedis, S.L. - Avda. de Barcelona 225
08750 Molins de Rei (Barcelona)

Publicación bimensual registrada el 14/2/03 con el número MI2003C/001404

hack·er (hăk'ər)

"Persona que se divierte explorando los detalles de los sistemas de programación y expandiendo sus capacidades, a diferencia de muchos usuarios que prefieren aprender solamente lo mínimo necesario."

INFIERNO INDISCRIMINADO

Recientemente se ha hecho tristemente famosa una cepa de virus, con el nombre genérico de MyDoom. Aunque se trata de virus que se han transmitido con velocidad meteórica, el "mérito" principal de estos bichos ha sido preparar y perpetrar ataques programados contra sedes de fabricantes como SCO y Microsoft.

El primero de los damnificados, SCO, es una empresa enzarzada en polémicas sobre la patria potestad nada menos que sobre Unix. Linux es uno de los principales implicados en la polémica. Podría muy bien ser que en el origen del virus se encuentre una venganza de algún linuxero disfrazado de caballero andante (y encapuchado).

El segundo de los atacados, Microsoft, presenta un cuadro distinto. El gigante de Redmond se ha destacado por apostar sin fisuras por su propia familia de sistemas Windows, mientras los demás sistemas operativos se han tratado sistemáticamente como la competencia. El problema es que su presencia masiva y, a menudo, sus métodos, le han proporcionado una posición de cuasi monopolio. No es menospreciable también la indignación que provoca poder apuntar con el dedo al ganador avasallador. Por estos motivos, probablemente, Microsoft ha sido el segundo objetivo del prolífico virus MyDoom.

En ambos casos, sin embargo, existen críticas comunes. El ataque, en su preparación, ha pasado por miles de ordenadores personales, ha transgredido su privacidad y su uso éticamente correcto, ha usurpado sus cuentas de correo, se ha instalado sin pedir permiso al usuario... Es decir, aun sin entrar en la execrable intención de resolver las cosas al estio del oeste, a tiros, MyDoom se ha comportado como un virus cualquiera: pisando los derechos de todos los usuarios a su paso. No hay nada de noble en este comportamiento. Una vez más, los programadores de virus han malgastado su indudable talento en perjuicio de todos.

redaccion@hacker-journal.com

UNA REVISTA PARA TODOS

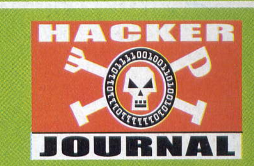






El mundo hacker se compone de algunas cosas simples y otras complicadas. Hay curiosos, lectores sin experiencia y expertos para los cuales el ordenador no tiene secretos. Cada artículo de Hacker Journal está marcado con una clave para cada nivel: NEWBIE (para quien comienza), MIDHACKING (para quien ya está dentro) y HARDHACKING (para quien no existen los secretos).

SUMARIO



Número 5-Marzo-Abril 2004

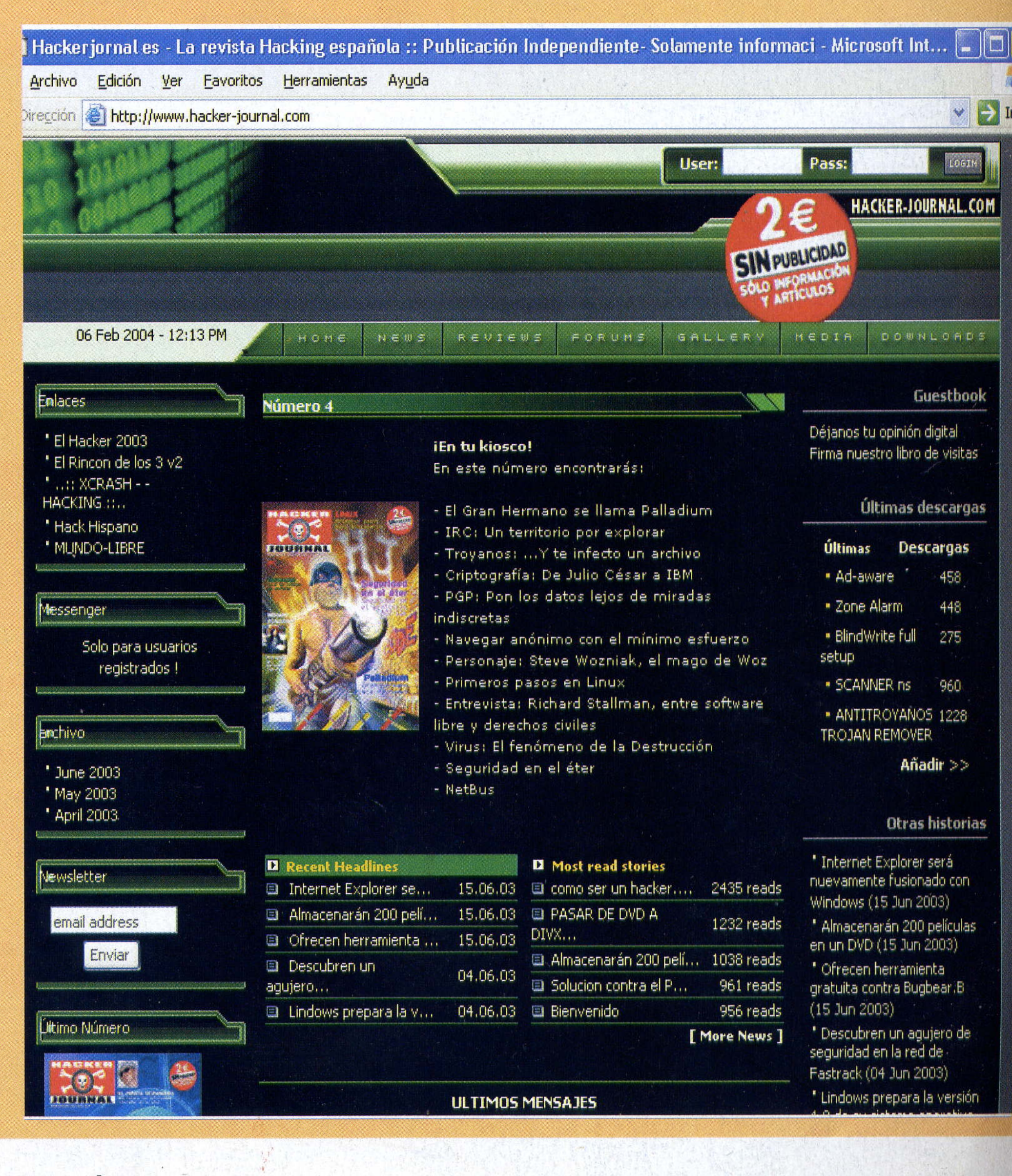
SITIO WEB

¡Bienvenidos a nuestro sitio web! Hemos cambiado el aspecto general del sitio, con un diseño más moderno y claro que esperamos que sea de vuestro agrado. Si hace tiempo que nos hacéis una visita, aprovechad ahora y enviadnos vuestra opinión a:

redaccion@hacker-journal.com

¡Tu opinión es importante!

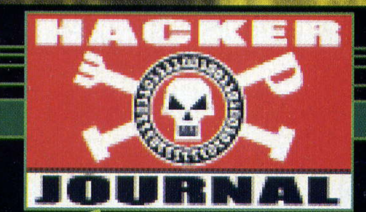
Visita nuestro sitio web:
www.hacker-journal.com



¡SECRET ZONE!

He aquí los códigos para acceder a la Secret Zone de nuestro sitio, donde podréis encontrar información y utilidades interesantes. Con algunos navegadores, puede ser necesario insertar dos veces los mismos códigos. No os detengáis al primer intento

user: secre5
password: 3studi0





mailto:

redaccion@hacker-journal.com

PALLADIUM

Salu2,

Me gustaria preguntar si palladium será realmente tan "fuerte" y seguro como se menciona. Además los ordenadores apple no tendran este problema no?

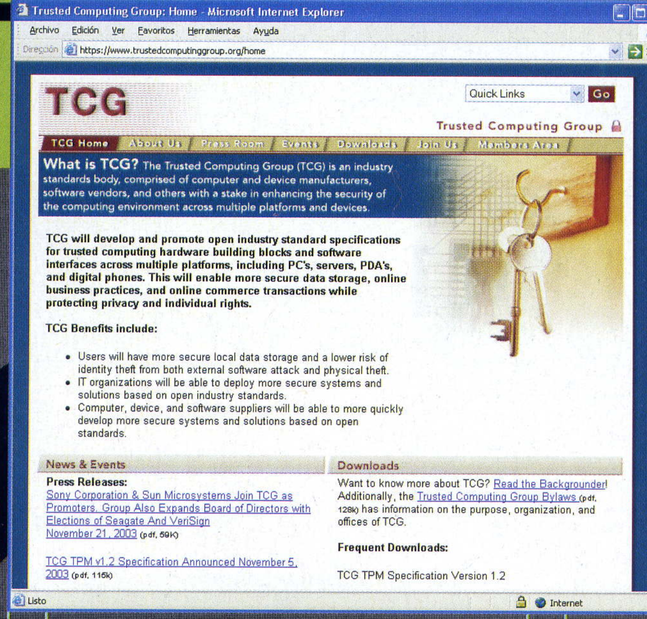
Gracias, vuestro lector,

Patrusquito

Ante todo, tenemos que puntualizar que Palladium ha cambiado de nombre. Ahora se denomina TCG, acrónimo de Trusted Computing Group. Si queréis saber cómo progresan sus trabajos, visitad el sitio web https://www.trustedcomputing-group.org/home.

Respecto a la fortaleza del invento, habida cuenta de los socios (AMD, Hewlett-Packard, IBM, Intel, Microsoft, Sony, Sun), parece que será tan seguro como quieran... No parece lógico pensar que si se diseña un sistema de cifrado para evitar que escape ningún componente del cerco, luego el mecanismo de protección, cifrado incluido, sea fácil de desactivar. La gran ventaja que tenemos los usuarios de a pie es que se trata del trabajo de un comité, compuesto por empresas que tanto pueden cooperar como competir. Por ello, cabe la posibilidad de que todo quede en una solución aplicada sólo a casos especiales, muy lejos de la universalidad que dicen perseguir.

Respecto a la inmunidad de los MacIntosh, ahora mismo parece asegurada, pero si Motorola o la propia Apple se apuntan al TCG, el panorama podría cambiar de pronto. Sería como mínimo curioso que Apple quedara al margen, que la iniciativa triunfara y que ello les diera el liderato en el mundo PC...



REGISTRADO

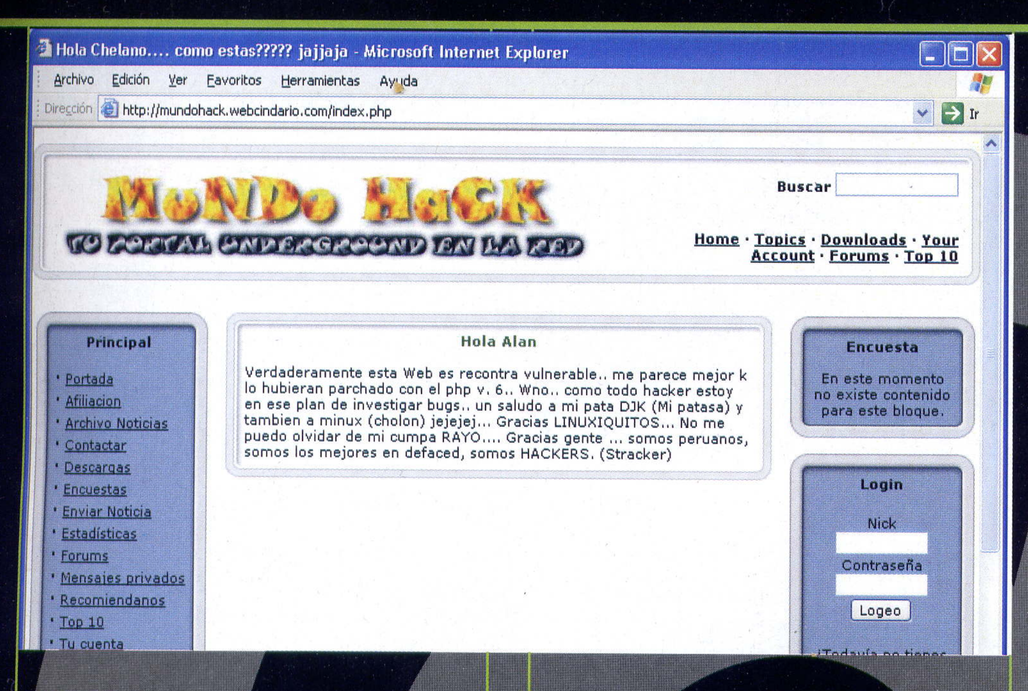
Compré el numero 4 de vuestra revista y me gusto mucho y me he registrado. Me preguntaría si podéis publicar mi página web por algún sitio, os lo agradecería mucho: www.galeon.com/pityworld y podeis poner en el numero 5 de vuestra revista los comandos del ms-dos "todos"

J. A. Sánchez

Aquí tienes la reseña que pedías. Tu sitio web resultará de interés para los aficionados a Warhammer. Te felicitamos por el diseño y el aspecto gráfico.

Respecto a incluir todos los comandos de MS-DOS, creemos que sería redundante, pues los manuales del sistema ya incluyen los comandos soportados. Para conocer comandos no documentados, la mejor recomendación es conseguir alguno de los magníficos libros que Peter Norton publicó hace años sobre este sistema operativo. En España aparecieron publicados por Anaya, pero actualmente son difíciles de encontrar. Tal vez más adelante incluiremos algún artículo sobre el tema. Lo cierto es que ahora hay más interés por Linux: los tiempos cambian.

PITYWORLD - Microsoft Internet Explorer
http://www.galeon.com/pityworld/
PITYWORLD
libros y reglas
PITYWORLD
programas y warhammer
fotos de warhammer
Mis aficiones
clan murciano de warhammer
socios
noticias
enlaces
batallas
FORO
WORLD MAP



HOLA DE NUEVO

¿Seríais tan amables de poner un manual en vuestra web aunque sólo sea un enlace o en vuestra revista cómo se utilizan los lenjuages de programacion visual basic, java....

J. A. Sánchez

¡El tema que propones es absolutamente mastodóntico! Si te inicias en la programación, será mejor que empieces por seleccionar un lenguaje y, cuando empieces a sentirte cómodo con él, puedes ir probando otras alternativas.
Visual Basic es una opción adecuada para empezar, pero tropieza con un par de problemas: es de Microsoft y sólo sirve para Windows, y es un lenguaje híbrido y algo caótico. El lenguaje Java (http://java.sun.com) es una opción más seria, es lo más transportable que existe actualmente y cuenta con una orientación a objetos modélica. Si vas a por todas, deberías considerarlo seriamente.
Otra alternativa interesante es Delphi, de Borland (www.borland.com), que se basa en el lenguaje Pascal con orientación a objetos y cuenta con un entorno gráfico de programación. Está disponible para Windows y Linux (como Kylix).

DEFACED

Antes de nada felicitaros por esa peaxo revista que os currais día a día y que cada vez tiene mas adeptos que se enganchan enseguida. Leo vuestra revista desde el número 1, y los tengo todos los consecutivos. Me gustaría si es posible que mi web aparezca en la revista, es de contenido underground-hack, que sigue día a día prosperando, es http://mundohack.webcindario.com . Muchas gracias. Ya estoy esperando que el próximo número llegue al kiosco.

iLLiCe

Aquí está tu propuesta, aunque es difícil hacer una valoración porque ¡parece haber sufrido un ataque defaced! No nos cansaremos de decir que una cosa es buscar y resolver fallos de seguridad, y otra muy distinta cargarse el trabajo de la gente para firmar la "broma". Amigo lector, lamentamos el ataque sufrido, y aquí nos hacemos eco de tu desgracia, que sentimos como propia. Por el bien de todos los hackers, por favor, señores gamberros: ¡maduren! Esperamos que nos comuniques cuando hayas podido resolver el problema. Así podremos incluir alguna imagen y una valoración del sitio web a toda vela. ¡Ánimo!

VIRUS

Nuevo virus detectado: Mydoom.A
Tened precaución
Síntomas:
Abre el bloc de notas de Windows "notepad.exe" y muestra en él un texto basura.
Propagación:
Mydoom.A se propaga enviándose por correo electrónico y copiándose en los directorios compartidos de la herramienta P2P Kazaa.
Dicho virus busca direcciones de correo electrónico en los ficheros del equipo que tengan las siguientes extensiones: .htm, .sht, .php, .asp, .dbx, .tbb, .adb, .pl, .wab, .txt
Se envía por correo electrónico utilizando su propio motor SMTP (es decir, no hace falta que nosotros enviemos ningún correo electrónico para propagarlo, ya se encarga el solito).
El contenido del mensaje varía, aunque las frases que lo componen son:
Asunto (cualquiera de los siguientes):
test
hi
hello
Mail Delivery System
Mail Transaction Failed
Server Report
Status
Error
Cuerpo (cualquiera de los siguientes):
Mail Transaction Failed. Partial message is available.
The message contains Unicode characters and has been sent as a binary attachment.
The message cannot be represented in 7-bit ASCII encoding and has been sent as a binary attachment.
Fichero adjunto:
nombre (cualquiera de los siguientes):
document, readme, doc, text, file, data, test, message, body
extensión (cualquiera de las siguientes):
pif, scr, exe, cmd, bat, zip
No olvideis la importancia de no abrir ficheros adjuntos con las extensiones que se indican ahí. Y en cualquier caso, no abrir ficheros adjuntos como norma general (salvo total confianza).
Suele ser una buena idea desconfiar sobre todo de aquellos mensajes cuyo titulo, texto, etc estén en inglés.

Glasnost

Pues eso.

NEWS

HOT!

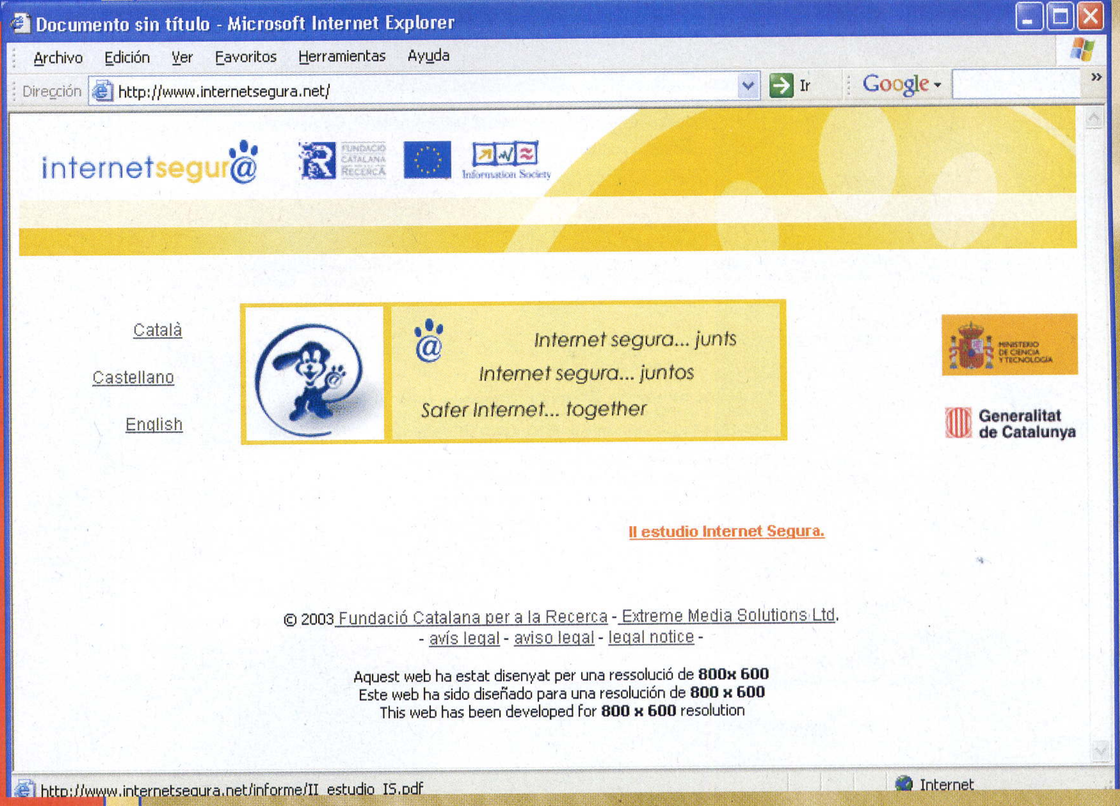
MICROSOFT CRECE UN 14% EN ESPAÑA

La cifra de negocio de la filial de Microsoft en España alcanzó los 319,9 millones de euros en 2003, un 14% más que en el ejercicio anterior.
Las ventas de nuevas licencias de la última versión de su sistema operativo Windows XP crecieron un 36%, por encima del 28% que aumentó el mercado de ordenadores en España, según datos de IDC. La nueva versión de Windows para empresas, Windows Server 2003, ha aportado una mejora superior al 26% en los ingresos de la división de servidores.
Por su parte, el paquete ofimático Office ha incrementado su facturación un 21%. Microsoft ha incrementado su plantilla un 7,5% en el último año y emplea a 403 personas en España.

INTERNET AGRARIA

La iniciativa Internet Rural pretende dar acceso a Internet de banda ancha a más de tres millones de ciudadanos de 1.600 municipios. El programa Internet Rural va a suponer una inversión total de treinta millones de euros. El ministro de Agricultura, Pesca y Alimentación, Miguel Arias, y el de Ciencia y Tecnología, Juan Costa, ya han inaugurado en Monteagudo de las Vicarías, municipio de 288 habitantes de la provincia de Soria, uno de los 34 telecentros que el Programa Internet Rural está instalando en la provincia hasta abril de 2004. Se trata de un centro de acceso público a Internet, gratuito para todos sus vecinos, y que cuenta con las últimas tecnologías de navegación por satélite.
Además de terminales de uso público con acceso a Internet de última generación vía satélite, el telecentro dispone de un Centro de Atención Técnica a Usuarios accesible mediante llamada telefónica a un número 902 o del correo electrónico. Se trata de un lugar público en el que los usuarios podrán utilizar sus propios equipos para navegar por Internet, contribuyendo así a la difusión de la Red.

DÍA INTERNACIONAL PARA UNA INTERNET SEGURA



Un total de dieciséis países de la Unión Europea celebraron el día 6 de febrero el Día Internacional para una Internet Segura, promovido por el programa Internet Segura -www.internetsegura.net-, una iniciativa del proyecto europeo SafeBorders en el marco del programa Safer Internet de la Comisión Europea. Esta jornada se celebró en Australia, Austria, Alemania, Bélgica, Dinamarca, España, Francia, Grecia, Irlanda, Islandia, Italia, Luxemburgo, Noruega, Países Bajos, Portugal, Reino Unido y Suecia, con el objetivo de garantizar el derecho de los niños a disfrutar de una Red segura.
En el sitio Internetsegura.net, un servicio gratuito, podéis informaros sobre la seguridad de los menores en Internet.
Se trata de una web dirigida a familias, maestros y otras personas que trabajen con o sean responsables de menores, así como también a organizaciones que trabajan para la infancia y adolescencia (administraciones públicas, bibliotecas, ONG, etc.).

NUEVOS PENTIUM4 DE 90 NANÓMETROS

Llegan al mercado los nuevos Pentium4 con tecnología de 90 nanómetros. Estos procesadores se encuentran entre seis nuevos productos ofrecidos en la línea de chips de escritorio de Intel, los que traen nuevas características y alto rendimiento a una extensa gama de usuarios de PC.
La tecnología de proceso de 90 nm (un nanómetro es una billonésima parte de un metro) es el proceso de fabricación de semiconductores más avanzado de la industria, construido exclusivamente en obleas de 300 mm. Este nuevo proceso combina mayor rendimiento, transistores de menor consumo de energía, silicio forzado e interconectores de cobre de alta velocidad. Esta es la primera vez que se integran todas estas tecnologías en un único proceso de fabricación.
Los procesadores Intel Pentium 4 construidos en base al proceso de 90 nm conservan las capacidades multi-tarea de la Tecnología Hyper-Threading (HT), e incluyen nuevas características como la microarquitectura Intel NetBurst mejorada, un mayor cache Nivel 2 (L2) de 1MB y 13 nuevas instrucciones.
Además de los cuatro procesadores fabricados en base a la tecnología de proceso de 90 nm, Intel agregó una versión de 3,40 GHz del procesador Intel Pentium 4 con soporte de Tecnología HT basado en la tecnología de proceso de 0,13 micrones a su familia de procesadores de escritorio.

GOOGLE ES LA MEJOR MARCA



Google, el principal proveedor de búsqueda en Internet y que planea entrar en bolsa este año, obtuvo un espaldarazo al ser considerado por segunda vez consecutiva "marca del año" por la empresa consultora Interbrand.

Por su parte, la empresa de computadoras Apple nuevamente obtuvo el segundo lugar del ranking de marcas de alto impacto, mientras que el automóvil Mini subió desde el puesto número once al tres.

Google basa su éxito en su interfaz sobria pero eficaz y en la casi ausencia de enlaces publicitarios, lo que le ha convertido en el buscador preferido de los navegantes de la web.

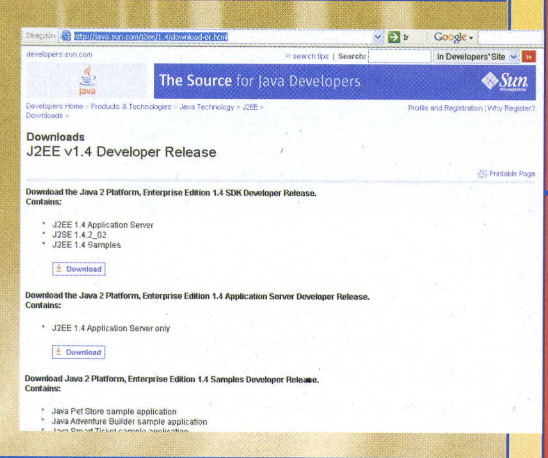
La empresa Interbrand, quien realizó la encuesta a cerca de 4.000 usuarios de 85 países a través de su sitio en Internet, dijo que Google tendrá que mantener su política de ofrecer una búsqueda "limpia, sencilla y creíble" a sus usuarios, si desea cotizar en bolsa.

SUN LANZA LA BETA DE JAVA 2 1.4

Sun Microsystems ha lanzado la versión beta de la plataforma Java 2, Standard Edition (J2SE) 1.5, con el código en clave de Project Tiger.

La versión beta de la última versión de J2SE, que engloba Sun Java Enterprise System, Java Studio Enterprise tools y Java Desktop, aparece con mejoras y actualizaciones en el lenguaje de programación Java para facilitar la programación a los desarrolladores.

Las mejoras están pensadas para incrementar la facilidad y la seguridad de la codificación en este lenguaje orientado a objetos. http://java.sun.com/j2ee/1.4/download-dr.html



AGUJEROS DE SEGURIDAD EN REAL PLAYER



RealNetworks ha reconocido que tres agujeros de seguridad que afectan a distintas versiones de su reproductor multimedia podrían permitir que un atacante cree archivos de vídeo o música corruptos de modo que, al ser reproducidos, le darían el control del PC de la víctima.

Los fallos pueden afectar a RealOne Player, RealOne Player versión 2, RealPlayer 8, RealPlayer 10 Beta, y los productos RealOne Enterprise.

El agujero de seguridad puede utilizarse mediante un archivo multimedia tratado especialmente, de diversos tipos: RealAudio (RAM), RealAudio Plugin (RPM), RealPix (RP), RealText (RT) o synchronized multimedia integration language (SMIL).

Las vulnerabilidades que actúan a través de un archivo multimedia han sido hasta ahora raramente aprovechadas. En mayo pasado, un fallo de Microsoft Windows Media Player permitía manipular los "skins" del programa, y dio lugar a un parche por parte del fabricante. RealNetworks proporciona instrucciones en su sitio Web para quienes quieran actualizar su software RealPlayer: http://www.service.real.com/help/faq/security/040123_player/EN/

HOT!

CONSECUENCIAS DE MYDOOM

La primera versión de Mydoom (MyDoom.A) tenía como propósito paralizar el lunes día 2 el sitio web de SCO y se salió con su propósito. Con más de un millón de equipos infectados en todo el mundo, muchos actuaron como atacantes en el mayor ataque de denegación de servicio de la historia.

Pero la segunda versión, MyDoom.B, que tenía como objetivo a Microsoft, no corrió la misma suerte. Según declaraciones de Microsoft, el ataque no se salió con la suya gracias a un gran esfuerzo técnico por parte de la compañía. Sin embargo, para valorar la situación, es preciso también tener presente que el virus MyDoom.B no consiguió infectar tantos ordenadores como sí consiguió la versión original.

SCO Y EL ORIGEN DE MYDOOM

Bruce Perens, de la organización Open Source, y codiseñador del sistema operativo de código abierto 'Linux', además de ser uno de los principales hackers de Linux, ha publicado en su página web sus sospechas de que existen motivos fundados para creer que la empresa SCO pueda estar tras el origen de MyDoom.

Según Perens: "Hemos reunido evidencias de que cometió perjurio en un proceso en curso en una corte que analiza la autoría de Linux". "Una compañía como SCO no dudaría en atacar su propio sitio de internet para desprestigiar a sus oponentes. Al parecer es un virus ensamblado por ciberdelicuentes (spammers), SCO u otros para difamar a los autores de Linux".

Perens afirma que SCO busca presentarse como una víctima ante la comunidad Linux, cuando en realidad es el auténtico agresor. Se trata desde luego de unas declaraciones que no se andan con chiquitas.

En esa línea, recomendó a los usuarios de 'Linux' que públicamente critiquen los ataques al tratarse de un intento por difamarles, así como a que prosigan apoyando la presencia visible del 'software' libre como una actividad positiva en el campo de la informática.

EL SÍNDROME DE CHINA

Spam, hackers de Estado, guerra digital y espionaje de masas: los inquietantes aspectos de la actividad informática en el país más poblado del mundo.

CHINA E INTERNET, UNA RELACIÓN POTENCIALMENTE PELIGROSA

Es la noche entre el sábado 31 de marzo y el domingo primero de abril del 2001. Una llamada hace saltar de la cama al vicepresidente americano Dick Cheney: es el estado mayor de la marina. Un avión espía nuestro , explica el almirante Housbound, ha sido abatido por los chinos hace pocas horas.

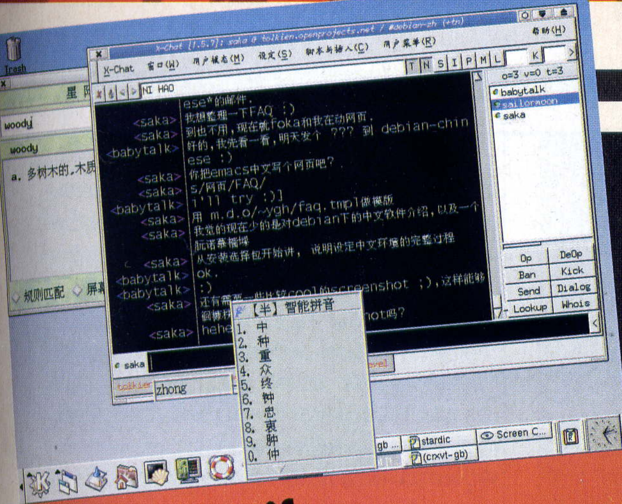
En realidad, **el avión, un gran cuadrimotor Ep-3, 24 hombres de pasaje, dotados con los más avanzados sistemas de vigilancia electrónica (léase "espionaje") ha sido interceptado al sur de la isla de Hainan, en el Golfo de Tonkin** (10 Km al sur según los chinos, 110 Km según los americanos). Un reconocimiento de rutina salido de la base de la Air Force de Okinawa, Japón, que de improviso se convierte en un drama. Dos cazas chinos flanquean el avión americano. el Ep-3 intenta una maniobra de evasiva, pero toca uno de los dos cazas (que cae y provoca la muerte de Wang Wei, el piloto) y -dañado- se ve obligado a aterrizar en la base militar china de Hainan. Bush, elegido presidente de los Estados Unidos, se moviliza rápidamente, pero China no se deja impresionar: al otro lado hay alguien más "duro" que el presidente tejano. Es Jiang Zemin, considerado un "duro" incluso por los generales de las fuerzas armadas chinas. Serán 11 días de tensión: por una parte los EE.UU. que reclaman la retirada de sus hombres y -sobre todo- la tecnología almacenada en su joyero volante para el espionaje electrónico; por la otra China, que pretende justicia e indemnizaciones por la violación del propio espacio aéreo y por la muerte de su piloto (además de querer curiosear entre las tecnologías americanas).



Mientras una flota de tres naves de guerra americanas se acerca al Mar de China meridional, sobre la mesa diplomática los chinos echan cuentas: para recuperar el avión los EE.UU deben comprometerse a no vender a Taiwan (la China nacionalista, en lucha contra la China continental comunista del fin de la Segunda Guerra Mundial) las nuevas tecnologías antimisiles, que limitarían la capacidad ofensiva china en caso de conflicto con este país. Al final, un compromiso diplomático desbloqueará la situación.

» Mientras, en la red...

Aun así, en los mismos días está teniendo lugar una guerra silenciosa que pocos han documentado. Entre el 2 de abril y el 9 del mismo mes, según un comunicado reservado de la sección de seguridad informática del Departamento de Estado americano, se dan



¿Como decís "spam" en Pequín?

Una enorme cantidad de mensajes publicitarios no deseados (spam) en circulación cada día llega de una forma u otra desde China. En parte se trata de mensajes mandados por las nacientes empresas privadas chinas, a la caza de relaciones comerciales con empresas extranjeras (mayormente americanas); estos mensajes a menudo están escritos en un inglés muy descarnado, o incluso en una de las lenguas chinas. No acostumbrados al uso de la red y desconocedores de la netiqueta, hordas de empresarios están acribillando a los occidentales con mensajes que, en el mejor de los casos, harán irritar a los potenciales clientes en lugar de alentarlos.
Más parecido a lo que conocemos habitualmente es el spam que, aunque originado en sitios y empresas occidentales, viene en realidad mandado apoyándose en servidores de correo chinos. En este caso suele ser difícil para el usuario corriente llegar al servidor de origen analizando la cabecera del mensaje, e incluso los mismos proveedores tienen problemas para gestionar la enorme mole de mensajes que llegan de la Gran Muralla. Algunos observadores sostienen que los servidores smtp chinos estarían muy poco protegidos, por lo que serían explotados ilegalmente por los auténticos "enviadotes" de spam... Pero lo que esta teoría no explica es cómo, en un sistema tan reglamentado y controlado, nadie se ha preocupado de identificar y retomar los administradores de los servidores que envían tantos mensajes. ¿Podemos preguntar qué pasaría si el objeto del spam fuese un sitio fuertemente crítico hacia el gobierno chino?

China en cifras

1300 millones de habitantes
9.596.960 kilómetros cuadrados de superficie
33,7 millones de usuarios de Internet
12 millones de ordenadores vendidos en 2001
90 millones de teléfonos móviles
200 millones de líneas telefónicas
Lenguas habladas: el 91, 9 % de la población habla el chino estándar o mandarín, derivado de un dialecto de Pequín, o el cantonés (Yue), el dialecto de Shangai (Wu), el Minbei (Fuzhou), el Minan (Taiwan), Xiang, Gan, varios dialectos Hakka. Además, las minorías étnicas (un 8,1 % de la población) hablan los dialectos Zhuang, Uygur, Hui, Yi, Tibetano, Miao, Manchu, Mongol, Buyi y Coreano.

cerca de 412 ataques informáticos "particulares". Por un lado, desconocidos y **hábiles informáticos americanos realizan cerca de 387 intrusiones de "elevado nivel y capacidad tecnológica" en el interior de sitios chinos**, para proclamar su patriotismo. Por el otro, **"piratas chinos han realizado al menos 25 violaciones informáticas" de sistemas estadounidenses, entre los que se encuentran el Departamento de Trabajo y el de Sanidad.**
No es la primera vez que China se convierte en protagonista de lo que se define como CyberWarfare, la Guerra Electrónica. Es la temida amenaza de la "Pearl Harbour digital", analizada en los Estados Unidos por los expertos militares de seguridad, y convertida pronto en la excusa oficial para la caza de hackers (sobre todo americanos y europeos) en curso del fin de los ochenta.
¿Pero China y los otros países el Extremo Oriente representaban realmente solamente un peligroso enemigo? A juzgar por los intereses económicos que sobre todo los Estados Unidos tienen en aquella área, se diría que no. Al fin del 2001 China ha entrado en la Organización Mundial del Comercio, y es considerada el mercado destinado a la mayor expansión, sobre todo en el campo electrónico. Es un continente entero, **poblado por una quinta parte de la población mundial** (1300 millones de personas), con 12 millones de ordenadores vendidos en el 2001, y 33,7 millones de usuarios de Internet que del 50% al año. Una auténtica bendición, con respecto a los agonizantes mercados tecnológicos occidentales.
En resumen, considerando el asunto desde el punto de vista industrial de las grandes empresas productoras de tecnología, China vive una situación única: coexisten viejas y nuevas tecnologías, se cruzan satélites, Internet, telefonía móvil, fibras ópticas e infraestructuras militares. Pero los usuarios son aún poquísimos y el coste del trabajo es extremadamente bajo. Quien gane el desafío del mercado chino, ganará todo el mundo. Quien pierda, perderá todo el mundo.
Pero China no se ha abierto a las tecnologías occidentales y a la llegada de las grandes multinacionales sin organizarse para defender su régimen interno.

>> Una red de mangas estrechas

La legislación prevé límites de varios tipos referentes a la apertura de nuevas fábricas con capital occidental, que deben obtener el *nihil obstat* del gobierno de Pequín, y el acceso a Internet por parte de la población está subyugado a una serie de reglamentos que en Europa ni siquiera son imaginables.
Desde hace dos años, se establece la **pena de muerte a quien sea reconocido culpable de haberse apropiado o de haber divulgado documentos de Estado** -por tanto cubiertos por el secreto- en Internet.
Es inútil decir que el concepto de "documento de Estado", aunque cubierto por el secreto, es interpretado en un modo bas-

Six/Four: comunicación anónima y segura

Fidonet y FredNet, aunque también las redes de base. La filosofía referente a las grassroots no es nueva, pero se desarrolla después del 4 de julio de 1989, el día de las masacres de la plaza Tiananmen, una de las páginas más negras de la historia reciente de China. El grupo de hackers Activismo, spin-off del colectivo Cult of the Dead Cow, decide realizar un protocolo que permita navegar, chatear e intercambiar archivos y emails sin dejar rastro. Una fuerte amenaza para la seguridad, se diría hoy, en realidad la única forma de seguridad posible para quien viva en un país donde el régimen trata de interceptar y censurar todas las formas de comunicación, incluso las electrónicas. En la base tecnológica del protocolo, Six/Four, hay un mix de VPN, tunneling, aproximación peer-to-peer y openproxy. Pronto se darán más detalles en el sitio hacktivismo.com, donde ya se puede encontrar una versión funcional de Camera/Shy, software de estenografía que permite esconder mensajes cifrados dentro de imágenes normales.

El principal autor del protocolo es The Mixter, un hacker alemán localizable en la dirección mister.void.ru. Mister, que es un personaje conocido en el ambiente hacker, también es autor de Tribe FloodNet, un programa usado a menudo para efectuar ataques dDoS.

tante amplio, y cualquier ciudadano chino que mande un email al extranjero con información considerada "secreta" (o "política" y "democrática") se arriesga efectivamente a la pena capital. Además en China, según Amnistía Internacional, las ejecuciones no son en absoluto un fenómeno raro.

>> The great (fire)wall of china

Desde el 1 de agosto de este año, además, **en China está en vigor una legislación que limita fuertemente el número y la estructura de los gestores de sitios, y los mantiene directamente bajo control gubernamental.**

Por si fuera poco, en los dos últimos años han sucedido los episodios de censura por parte del gobierno chino con respecto a Internet: los proveedores locales han sido obligados a impedir el acceso a series enteras de Ip, **en 2001 se ha impedido el acceso a Freenet** (servicio Ftp de intercambio de información sin censura) **y a los principales motores de búsqueda** (Google, Altavista, Yahoo, etc.). Aún más, en tres diferentes etapas el gobierno ha cerrado los Internet Cafés de la capital, punto de acceso para las grandes masas de estudiantes que frecuentan Pequín y que no pueden permitirse un ordenador y una conexión a Internet. En otras zonas, para acceder a los Internet Cafés hay que registrarse en la policía y obtener una tarjeta de reconocimiento, que permite **rastrear y registrar cada actividad realizada online por los ciudadanos**.

Sin contar la instalación de **sistemas análogos al americano Carnivore: box dedicados al filtraje de los paquetes Tcp/Ip instalados por ley en los servidores de suministradores de acceso**. En los EE.UU., a pesar del 11 de septiembre, la cuestión aún se discute; en China es una certeza matemática.

En resumen, si en el pasado China se defendió de los mongoles con la Gran Muralla, ahora el gobierno querría que el país se transformara en **una enorme Intranet cerrada por un cortafuegos**, con contenidos altamente controlados. Para esto, lucha incluso contra las principales empresas productoras de software: desde hace casi año y medio están en curso las **experimentaciones para basar las infraestructuras chinas en servidores y escritorios de entorno Linux**. La idea es que de esta forma es posible hacerse autónomos de Microsoft, y de las políticas de "seguridad" que el sistema operativo de Microsoft está realizando bajo el empujón del gobierno estadounidense. Tener una infraestructura no basada en Windows significa no estar expuestos, en caso de guerra comercial o electrónica, al riesgo de que el potencial enemigo, los EE.UU., también sea el posesor de uno de los recursos fundamentales: el sistema operativo de los ordenadores.

>> Vida dura para los hackers

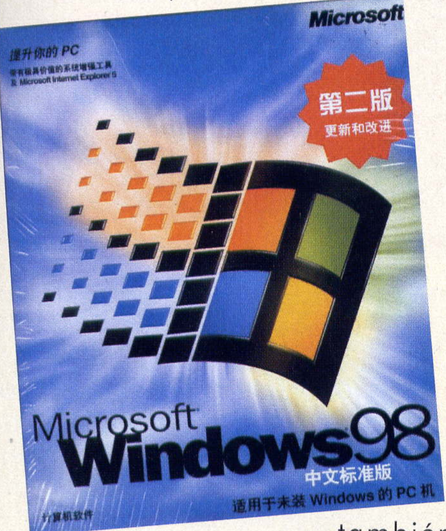
Pero el escenario hacker del Extremo Oriente no es menos vital que los occidentales, aunque esté fuertemente contaminado por el **omnipresente gobierno, que trata incluso de enrolar a los mejores talentos.**

Difíciles de individualizar, a menudo parte de los movimientos antagonistas del régimen de Pequín, los hackers chinos nacen sobre todo cerca de los grandes centros universitarios del país, como Hebei, Yenching, Tsinghua, Chaoyang, Soochow, Xiamen, Wuhan, Hunan, pero también en las áreas de mayor industrialización tecnológica, como Shangai y Hong Kong.

Su presencia se advierte como una amenaza nacional, y hemos visto que en algunos casos **esto se puede traducir**

en condenas durísimas, incluso en la pena capital. Durante los últimos meses han sido arrestados al menos 15 "presuntos hackers", a partir del arresto, en el distrito de Haidian (Pequín) en mayo del año pasado, de Lu Chun, **un muchacho de veintiún años culpable de haber robado un par de cuentas de una empresa y haberlos usado para navegar por Internet** (y dejar navegar a algunos de sus amigos) hasta el arresto del muchacho de diecisiete años Chi Yongshu, estudiante de secundaria en la provincia Heilongjiang (al noreste del país), culpable esta vez de **actos más complejos: difusión de virus, hurto de datos y tráfico ilícito online**. Por último, un hombre de 36 años empleado de una institución de crédito (Banca de comunicaciones de China), **acusado de haber robado de las cuentas corrientes de los clientes casi dos millones de yuans** (200.000 dólares) a partir de agosto de 1990, después de huir a Canadá y ser expulsado por las autoridades de este país, **fue condenado a muerte y ajusticiado.**

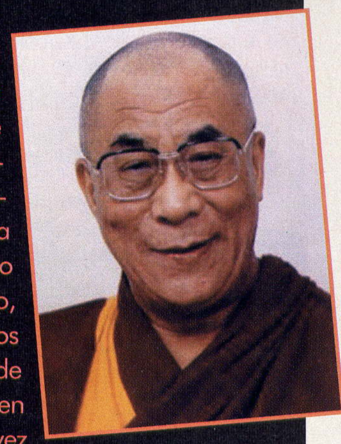
Los hackers,



también "heike", como se traduce fonéticamente la expresión inglesa al chino, aún así están allí. Y no son ladronzuelos, jovencitos que juegan con los passwords o soldados de la ciberarmada de Pequín. Varios grupos de hackers europeos y estadounidenses, que últimamente han confirmado que no están involucrados con los ataques que se han desencadenado desde Occidente contra los enemigos de los Estados Unidos como China, Corea del Norte e Irak (la última en declarar su extrañeza ha sido Legion of Underground) con el tiempo incluso han establecido contactos fuertes con sus colegas chinos. A su vez, el contacto ha significado una ayuda sustancial. **La comunidad hacker internacional, sensible -como es obvio- al tema de poder garantizar la propia privacidad delante de regímenes opresivos, ha ofrecido soluciones para quien vive en países como China**: software como Camera/Shy de Activismo y Six/Four para la creación de redes grassroot absolutamente anónimas, son regalos pensados no para proporcionar nuevas armas a los hackers "cautivos" y terroristas extranjeros, sino **para permitir el ejercicio de los más elementales derechos democráticos también a quien vive en países en los que esto no está permitido.**

Desde China, aparte de hackers éticos y combatientes para la democracia, llega mucho más que el virus de la gripe otoñal. **Cada año se cuentan al menos una decena de "cepas" virales informáticas procedentes (o así lo parece) del Extremo Oriente**. Por ejemplo, el Word 1i0n. Los mass-media, acostumbrados a hacer de cada hierba un fajo con el termino hacker, con el "peligro amarillo" se quedan literalmente a gusto. Aun así, la guerra subterránea entre presuntos hackers occidentales (sobre todo americanos) y chinos continúa. De dimensiones muy reducidas con respecto al conflicto entre "piratas" filopalestinos, el bombardeo a golpe de defeacement está en curso. Quizá en China también con la aprobación gubernamental, si no con su propia intención. Grupos como The Honker Union of China (Honker es una de las expresiones slang chinas para hacker) han declarado que quieren combatir "la arrogancia antichina" con todos los medios. Incluso con 80 defeacements consecutivos y el compromiso de otros 400 servidores.

Pequín contra la Red del Dalai Lama



"We are definitely under attack. This is not paranoia. Something very weird is going on, BEWARE", así iniciaba, el sábado 20 de abril de 2002, el preocupadísimo email de Anthony O'Brien, uno de los más asiduos frecuentadores de Tibet Support Groups-List (TSG-L), la principal red internacional de tibetanos y sostenedores de la lucha del pueblo tibetano contra la ocupación china del País de las Nieves. Qué cosa tan grave estaba sucediendo? Como se aclaró en el decurso de pocas horas, algunos hackers chinos habían conseguido, gracias a una abanicada de virus Trojan, apoderarse de los ordenadores de algunos de los más conocidos animadores de la lista y, a través de emails enviados a su nombre, entrar en docenas de otros ordenadores de inscritos a la TGS-L. Una vez fueron examinados por expertos de Symantec y Mcafee, estos virus resultaron ser extremamente sofisticados y enviados desde Pequín y de otras ciudades de la China Popular. Aunque el gobierno chino ha negado oficialmente tener nada que ver con este ataque masivo y coordinado, los tibetanos y sus amigos están absolutamente convencidos de que es imposible en un país como China, donde rige el más total control gubernamental sobre todos los aspectos de la comunicación, parta la comunidad de los hackers (que por otra parte es en general cualquier otra cosa que favorable al régimen) realizar una operación tan bien articulada y prolongada en el tiempo. Además todas la redes conectadas a los distintos aspectos de la disensión china (sindicalista clandestinos, intelectuales, adeptos a la Falun Gong, etc.) han comunicado a la TSG-L que han sido también sometidas a análogos ataques. Ahora la TSG-L está intentando equiparse para responder a la emergencia porque está claro que incluso en el Techo del Mundo y en el remoto Oriente los verdaderos juegos se dan en la red.

HACKER STORY

MISTERIO 23

Todos los elementos de la novela policíaca se encuentran en la historia de Karl Koch, el hacker alemán muerto en circunstancias misteriosas...

Un PC, una línea telefónica, un genio de los ordenadores un poco desequilibrado, una muerte misteriosa. Todos los elementos de la novela policíaca se encuentran en la historia de Karl Koch, el hacker alemán **muerto calcinado en su coche el 23 de mayo de 1989**, pocos días antes de comparecer en el tribunal por una historia todavía por comprender. Koch, genio rebelde, infancia difícil y adolescencia hecha de porros y coca, hizo del ordenador su vida. Y quizá, precisamente por el ordenador, la perdió.

>> Juegos peligrosos

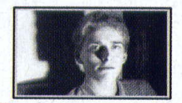
Cuando sus acciones de hackerismo lo empujaron a meterse en las redes informáticas estadounidenses, al principio solamente como un juego, las cosas se volvieron más gruesas que él, que Pengo y que aquel grupo de seguidores del Chaos Computer Club. Sí, **porque en una Alemania ocupada en la caída del muro de Berlín, este grupo de jovencísimos hackers decidió poner a disposición de la KGB todo el material recogido**. ¿Material importante? Probablemente no. Pero la historia de Koch no puede no resultar fascinante. El enamoramiento con Hagbard Celine, figura central de la novela Los Iluminados I, no es simplemente el querer buscar una figura para mitificar a toda costa. Tiene sólo 14 años, Karl, cuando lee una novela que le ha regalado, quizá por error, su padre alcohólico. **Los Iluminados son una potente congregación secreta que trata de provocar la tercera guerra mundial**; Hagbard Celine trata de combatirlos. "Él es un genio loco -recuerda a menudo Karl- altamente cualificado, que puede realizar una serie de actividades que van de la jurisprudencia a la ingeniería". Decide hacerse pirata, Hagbard, y viajar en su submarino dorado. Se vale de la colaboración de un ordenador (Fuckup) que calcula sin parar el destino del mundo. Un personaje fascinante, que lo acompañará en su crecimiento. En pocos años Karl pierde a su madre y a su padre. Con la herencia del padre compra un ordenador potente que le permite, finalmente, "entrar como Dios manda en la escena de los ordenadores".



K23, la historia del hacker Karl Koch, es el libro de Hans-Christian Schmidt y Michael Gutmann escrito sobre el caso del joven hacker muerto el 23 de mayo de 1989. De estas páginas se ha sacado también la película "23", enteramente dedicada al mundo hacker.

Curiosidad

Un número misterioso, anarquista: el 23. Karl Koch murió el 23 de mayo a los 23 años. Todos los grandes anarquistas han muerto en un día 23, como escribió "Der Spiegel". Este número atrajo mucho a Karl en su estudio sobre las conspiraciones. Pensó, por ejemplo, en el homicidio del primer ministro sueco Olof Palme, acaecido una noche a las 23 y 23. La idea última que tenía Karl era que todos, sin saberlo, servimos a los objetivos de los Iluminados. El número 23 proviene de la novela de Robert Anton Wilson convertido en culto para el hacker alemán, que reencontró el 23 en la historia (¡23 Skidoo!) del escritor Burroughs, amigo de Wilson. Burroughs, una vez, contó que había conocido a un marinero que navegaba desde hacía 23 años y que presumía de no haber tenido nunca un accidente: aquel mismo día el trasbordador en el que viajaba este marino se hundió. Por la noche Burroughs encendió la radio para escuchar todas las noticias relacionadas con el suceso y oyó otra noticia: un avión se había precipitado sobre la ruta Nueva York-Miami: ¡el vuelo estaba registrado con el número 23! Aún más: el 23-5-1949 entró en vigor la constitución de la República Federal de Alemania, hasta el 23-5-1999. ¿Sabías que el 23-5 resultaron muertos Bonnie & Clyde y el magistrado Giovanni Falcone? Finalmente, el día del inicio de la retoma del 23 murió Burroughs. Un número, un destino.



In Erinnerung an Karl Koch

-- HAGBARD CELINE --

* 22.07.1965
† 23.05.1989

Una entrada fuerte, impresionante. Karl pasa las noches delante del monitor, por la mañana hay montañas de papel cerca de la impresora. **Se nutre de café y zumos multivitamínicos, fuma cigarros y del hachís se pasa a drogas más duras. El suelo es una alfombra de disquetes y matrices para grabar tarjetas**. ¿Qué estaba haciendo? En qué estaba trabajando aquel Karl Koch, a un paso de la mayoría de edad, ya convertido simplemente en "Hagbard" en el mundo de los informáticos? Los actos heroicos de los hackers americanos ya son bien conocidos incluso en Alemania y en el 84 nació el Chaos Computer Club. ¿Con qué objetivo? "Hacer servicios de patrulla al margen de lo irreconocible, sensibilizando la opinión pública sobre el problema de la seguridad de los datos... comportándose de manera ofensiva pero amistosa, subrayando cómo los hackers muestran precisamente los puntos débiles en el sector de la seguridad". Escribe Karl en una autobiografía: "con un par de excepciones vivo en el aislamiento de mi ambiente y de mi búsqueda de amistad. Las sesiones de hackerismo duran días y noches. Me comunico, la mayoría de las veces, a través del ordenador... dedico mi tiempo sólo al ordenador." Las sesiones de hackerismo se hacen cada vez más frecuentes. Cuando empieza la acción de hacking en el centro de investigación nuclear Fermilab de Chicago, Hagbard está en primerísima línea. El FBI lo descubre, pero no hay pruebas y el vacío legislativo hace el resto, para una materia legal aún por descubrir. El banco de datos Optimis del Pentágono, luego, se convierte en el objetivo favorito de los hackers, pero **Karl piensa en otra cosa: el Norad, o centro de control estratégico para la defensa aérea de los EE.UU**. Quiere entrar en el sistema como en la película Juegos de guerra. Descubre el acceso y, de acuerdo con el hacker Urmel, decide... olvidarlo. "Habría sido un fracaso".

>> Una misión

Pero las largas noches pasadas delante del ordenador lo convencen de una cosa: **tiene una misión personal en la inminente guerra informática entre las potencias mundiales**. Esta idea, madurada y corroborada por los sucesos del hacking nocturno, cuando todos los ordenadores son aparentemente inaccesibles, resultan, en realidad, fáciles de"desmontar". Los hackers salen poco a poco al descubierto, incluso con el objetivo de alejar las acusaciones de que son sólo unos criminales: durante la feria informática Cebit de Hannover, así, Hagbard tiene un rostro incluso para los periodistas: se mete en el escritorio, delante de un ordenador, y empieza a violar las líneas de correos alemanas y escruta los datos de la Universidad de Caltec, en California. Los periódicos empiezan a centrarse cada vez más en los casos de esta docena de hackers alemanes capaces de entrar en el ordenador central de la NASA. **Y cuando a alguien se le ocurre dirigirse a los servicios secretos rusos, el juego dura poco**. Llega el dinero para Karl, Pengo, Dob y Pedro, pero llegan también los problemas. Karl termina en un ángulo, cada vez más aislado. Es constantemente seguido por los servicios secretos del Este y naufraga en sus pensamientos sobre los Iluminados. Trata de salir a flote, busca dinero, intenta encontrar el scoop para periodistas dispuestos a todo... Sólo encuentra la muerte. Suicidio, se escribe en los documentos oficiales. **Lo han suicidado, dicen algunos**. El fin de un hacker. Desequilibrado, pero genial.

Homepage
Über mich
EDV-Profil
Projekte
Interessantes
EDV-Klassiker
Links ins Web
E-Mail an mich
Zurück

Karl "Hagbard Celine" Koch

Der Anlaß

Mitte 1997 erreichte mich die Information, daß ein Spielfilm über den sogenannten KGB-Hack, der 1989 für viel Wirbel in der Presse sorgte, gedreht wird. Speziell sollte es in dem Film um die Geschichte von Karl Koch, einem der beteiligten Hacker, gehen.
Da ich Karl bis zu seinem Tod kannte, ließ diese Information viele Situationen aus der Zeit von 1985 bis 1989 wieder in mir wach werden.
Karl starb viel zu früh am 23.05.1989 mit nur 23 Jahren durch eine vermutliche Selbstverbrennung. Sein Körper wurde erst einige Tage später gefunden. Ich erfuhr von seinem Tod erst am Sonnabend, den 03.06.1989, durch die Tageszeitung. Für den Freitag, den 26., waren wir noch bei mir verabredet gewesen. Sein plötzlicher Tod hat mich und viele andere aus seinem Bekanntenkreis schockiert und ratlos gemacht.



REFERENCIAS

http://www.hagbard-celine.de/
http://www.decoder.it
http://www.shake.it
http://www.mtr.webconcept.de/D/KarlKoch.html
http://www.ccc.de/



Chaos Computer Club e.V.
KABELSALAT IST GESUND
suche

[Themen | antworten | Impressum | Sprache/language]

Surfen und keiner horcht mit. HTTPS macht's möglich.

/Aktuelles
»Chaos Realitäts Dienst
»Chaos Updates

/Themen
»Hackerethik
»Zensur
»Funknetze
»Cybercrime-Konvention
»weitere Themen

/CCC Regional
»ERFA-Kreise und Chaostreffs
»Veranstaltungen

Chaos Computer Club

Die Datenschleuder #077

18. Juni 2002, *arne*

Gerade frisch aus der Druckerei erscheint in dieser Woche die Datenschleuder #077.

Chaos-Bildungswerk Hamburg: Gadget-Day am 13.06.2002

08. Juni 2002, *ccc-hamburg*

Was ist Dein liebstes Spielzeug?

KPNQwest NOC Besetzung

Erklärung gegen die Einschränkung der Informationsfreiheit

/ChaosWeb
CCC Berlin
CCC Bielefeld
Chaosdorf/Düsseldorf
CCC Hamburg
Köln
CCC Ulm

LOS FUNDAMENTOS DE LA CRIPTOGRAFÍA MODERNA

EL CIFRADO DE DOBLE CLAVE

No, no nos estamos refiriendo a la "doble vuelta de llave" con que se cierra la puerta de casa para estar seguros, sino al algoritmo matemático que en los años setenta revolucionó la ciencia del cifrado de mensajes.

En un número pasado hablamos sobre los albores de la criptografía y de los métodos que se han impuesto hasta los primeros decenios después de la Segunda Guerra Mundial. En 1976 se publicó un estudio titulado "New Directions in Cryptography". Los autores eran Whitfield Diffide y Martin Hellman, e hipotetizaban **un sistema que permitiera tener dos claves: una pública para cifrar los mensajes y una privada para descifrarlos.** Estas dos claves tenían que estar hechas para poder impedir reconstruir una conociendo la otra. Al año siguiente tres investigadores del MIT consiguieron identificar un algoritmo aplicable a esta teoría. Se llamaban Ronald Rivest, Adi Shamir y Len Adleman y bautizaron el algoritmo RSA, aun hoy usado en distintas variantes con un grado de seguridad prácticamente absoluto.
Todo se basa en algunos conceptos matemáticos, a decir verdad muy simples. Con dos números primos, es una operación banal establecer su producto, pero una vez dado el producto es casi imposible volver a subir a los números primos originarios, especialmente si los números primos son muy altos. Esto pasa porque **no existe ninguna regla para descomponer en factores un número dado, y hace falta proceder por imaginación e intentos.** Antes de que alguien se ponga manos a la obra, hace falta considerar que en los años 90, para descodificar sin la clave un mensaje con clave de 128 bits, **habría que usar más de 1600 ordenadores durante un tiempo de 8 meses.**

Actualmente los programas para el cifrado asimétrico usan claves que superan los 2048 bits. En este contexto la clave privada de un sistema asimétrico contiene los números ya descompuestos mientras que la pública contiene su producto. Por esto es imposible volver a una clave privada partiendo de la pública.
El problema real de este tipo de cifrado es sobretodo que, incluso con la clave, la operación de codificado y descodificado es extremamente lenta: hasta 1000 veces más lenta que un sistema tradicional. **Para resolver el problema han nacido los sistemas mixtos que mezclan las ventajas de los métodos tradicionales con los del sistema de clave asimétrica.** Cogemos por ejemplo un

La apertura de un texto cifrado con PGP no da motivos para un análisis, si no es la presencia de las siglas PGP iniciales. En realidad, para operar sobre un texto de este tipo se necesitan programas bastante complejos, una serie de ordenadores potentes y una buena dosis de paciencia, visto que el sistema de codificación de PGP puede requerir décadas para volver a una clave simple.




ARPR versione 1.11 - Registrato

Advanced RAR Password Recovery

Apri | Salva | Avvia! | Ferma | Benchmark | Guida | Info | Esci

File RAR crittografato: C:\WINDOWS\Desktop\DivX\avi_

Tipo di attacco: Forza bruta / Maschera / Dizionario

Intervallo | Lunghezza | Dizionario | Salvataggio automatico | Opzioni | Advanced

Opzioni — Priorità: Background / Alta — Aggiornamento — Registrazione

Riduci ad icona nel system tray

Abilita il log nel file arpr.log

Lingua: Italiano

Aggiorna l'indicatore d'avanzamento ogni 500 ms

Risultato del Benchmark

Statistiche su Advanced RAR Password Recovery:

Password da eleborare	853.058.371.539.159.299
Tempo d'esecuzione	Più di un anno
Velocità media (password per secondo)	625

OK

La descodificación mediante la fuerza bruta requiere bastante tiempo, especialmente por parte de personas solas. Incluso si este tipo de descodificación se hace sobre archivos que no tienen sistema de criptografía fuerte puede resultar bastante arduo. Pero no nos dejemos engañar porque estas operaciones en general son llevadas a cabo por gobiernos capaces de "probar" decenas de millones de passwords y no sólo el millar de passwords por segundo de un ordenador normal.

mensaje que hay que transferir de A a B. con un sistema tradicional se codifica con cierta clave y se transfiere de A a B pero la clave debe estar ya en posesión de B o hay que comunicársela usando un canal distinto del que se use para enviar el mensaje (y aquí está el primer gran riesgo: si la clave es interceptada todo el sistema de criptografía se hunde miserablemente). Con una codificación de clave asimétrica, en cambio, A puede codificar el mensaje usando la clave pública de B y B lo descodificará con su clave privada. El problema es que B empleará mucho tiempo para reconstruir todo el mensaje porque el uso del sistema asimétrico requiere más tiempo.

La solución ha sido mezclar los dos métodos. A codifica el mensaje usando un sistema tradicional como IDEA y con una clave completamente casual, generada automáticamente. Luego la clave se codifica con la clave pública de B, para hacerlo ilegible. Todo esto se envía a B que, para leer el mensaje, deberá descodificar la clave temporal mediante su clave privada y luego podrá descodificar el mensaje propiamente usando la clave que ha reconstruido.

Hoy el programa de criptografía más usado en el mundo es PGP, creado por el americano Phil Zimmermann, que usa el sistema mixto para la codificación de mensajes. Este sistema es tan seguro que Zimmermann ha sido acusado en los EE.UU. de haber violado la seguridad nacional, difundiendo un sistema de cifrado que no puede ser controlado por el gobierno de los EE.UU. Fue exculpado después de dos años y medio de dura batalla y actualmente no se sabe de nadie que haya conseguido descodificar los mensajes criptografiados usando PGP. La pregunta que inquieta a tantos paladines de la privacidad es: "¿no se sabe de nadie porque nadie la ha descifrado, o porque quien la ha descifrado no tiene ningún interés en decirlo?"

El algoritmo RSA

Se trata de una función particular, llamada "no reversible", porque de su resultado no es posible volver a los valores de entrada. Un poco como si mezcláramos los ingredientes de un pastel. Sería un poco difícil, partiendo del pastel, dividir los ingredientes originales entre ellos.

En la práctica se escogen dos números con algunos centenares de cifras decimales (escogidas por casualidad) que sean números primos. Para hacerlo se usa el test de Fermat. Luego se determina el producto de los dos números pares inmediatamente inferiores. Si A y B son los dos números se tendrá f1=A*B y f2=(A-1)*(B-1). Luego hay que escoger un valor C que sea primo con respecto al resultado de f2. O sea, C no debe tener factores primos n relación con f2. Para terminar, se encuentra un número, llamémosle D, que multiplicado por C y dividido por el resultado de f2, dé como residuo de la división 1. Haciendo un ejemplo con números pequeños tendremos:

A=7 y B=5

f1=35 y f2=24

24 puede ser descompuesto como 3*2*2*2, por lo que hay que encontrar un número que no tenga estos divisores. Pongamos C=7.

Por esto el resto de la operación D*7/24 debe ser igual a 1. Podemos poner D=7 (7*7/24=2, con resto 1).

El cifrado se hace dividiendo el texto en bloques con una longitud no estándar porque la longitud de los bloques corresponde al más grande entero X que satisface la ecuación 2^X<f1. En nuestro ejemplo, 2^5=32, por tanto el texto se dividirá en bloques de 5 bits.

Cada bloque Z se cifra calculando el resto de la división Z^D/f1. El descifrado de un bloque, Zc, se obtiene calculando el resto de la división Zc^C/f1.

Está claro que en la clave pública está insertado tanto el valor de D como el de f1, pero también está claro que para volver al valor de C, indispensable para descodificar, hace falta mucho trabajo. De manera específica, el trabajo es el de encontrar los números A y B conociendo sólo el producto. El nombre del problema es "factorización de los números primos" y no existe actualmente ningún instrumento matemático directo para resolverlo con números de una cierta magnitud.

Con las claves actualmente usadas, a 2048 bits, el tiempo necesario para reventar este sistema de protección puede llegar a algunos cientos de años.

¿Quién ha dejado la puerta abierta?

¿Crees que estás seguro porque no tienes un servidor Web, Ftp o Telnet en ejecución? ¿Estás seguro de que no hay ningún otro puerto abierto?

Los puertos del sistema son canales a través de los cuales se da el intercambio de datos del host local hacia un procesador y hacia un dispositivo de red cualquiera. Su número es muy grande (65546) y de base se han dividido en dos categorías principales: los puertos conocidos y los desconocidos.

Los puertos conocidos son los primeros 1024 y se asocian a los servicios del sistema; los puertos desconocidos son todos los que siguen, **del 1025 en adelante y que son normalmente asociados a servicios no identificados**, o que no forman parte del sistema en sí. Por desgracia, aparte de algunos usos más que legítimos, estos "servicios" a menudo se reagrupan en tres categorías: **virus, gusanos y caballos de Troya.**

Los virus son programas que se autorreproducen y se difunden usando otras aplicaciones en el interior del ordenador que lo hospeda. Los gusanos funcionan como los virus con la diferencia de que se propagan a través de la red.

Los caballos de Troya son aplicaciones que enmascaran, bajo la apariencia de un programa útil, un código dañino que puede desarrollar varias actividades en el interior del PC.

>> Damos los números

Veamos ahora al detalle los más "conocidos" entre los puertos desconocidos y los peligros que pueden representar. Como verás, al inicio de la lista hay también algunos puertos inferiores al 1024 (puertos conocidos) que pueden ser usados en modo fraudulento por programas distintos de aquellos para los que han sido pensados y reservados.

Puerto 21, 5400
Programas como Blade Runner, FTP trojan, Invisible FTP o WinCrash usan el puerto 21 para crear variantes peligrosas del servicio FTP; estas variantes pueden ser controladas remotamente y permiten la carga y descarga de archivos y programas.

Puerto 23
A veces es explotado por el servicio TTS, que funciona como un programa de emulación de terminal que opera de manera invisible (un servidor telnet oculto). Una vez conectados en modalidad telnet clásica se pueden impartir comandos para ejecutar en el sistema atacado.

Puerto 25, 110
Muchas aplicaciones a primera vista inocuas que simulan fuegos artificiales o la explosión de un tapón de champán esconden demonios que pueden robar passwords de sistemas y enviarlos vía email. Si no estás usando programas de correo pero ves abiertos estos puertos, hay algo que no cuadra.

Puerto 31, 456, 3129, 40421
Servicios como Hackers Paradise usan sobre todo el puerto 31 para adquirir el control del sistema y para modificar el registro de configuración.

Puerto 41, 2140, 3150, 60000
Un daemon conocido como Deep Throat ofrece enormes posibilidades de gestión remota del ordenador, entre las que hay: servidor FTP, administración remota, captura de pantalla, gestión de los procesos en ejecución.

Puerto 113
El servicio Kazimas es un gusano que se autodifunde a través del mIRC. Una vez infectado el aparato, se autorreproduce y cambia el archivo de configuración del mismo mIRC.

Puerto 119
El famosísimo Happy 99 a primera vista parece un inocuo pasatiempo lleno de fuegos de artificio, pero en realidad esconde un peligrosísimo programa de sustracción de password, mail spamming y ataques DoS.

Puerto 555, 9989
Programas como NeTAdmin y Stealth Spy tienen como objetivo destruir el sistema infectado después de reproducirse y autodestruirse.

Puerto 1010, 1015




El servicio conocido como Doly Trojan es un caballo de Troya capaz de adquirir completamente el control remoto del ordenador infectado.

Puerto 1024, 31338
El servicio NetSpy es uno de los más conocidos, puede espiar la actividad en el interior de un PC y gestionarla remotamente. Incluso puede bloquear el botón Inicio y esconder la barra de aplicaciones.

Puerto 1234
El daemon Ultors es otro troyano que permite tomar el control remoto del ordenador infectado.

Puerto 1600
Es asociado a un troyano de diseño muy simple, el Shivka-Burka, que sólo tiene la función de transferir archivos.

Puerto 1999
El servicio BackDoor fue uno de los primeros caballos de Troya con un backdoor asociado. Ofrece varias posibilidades de control remoto del PC, como control del ratón, vídeo, tareas, chat y mensajería.

Puerto 2115
Bugs es un programa de acceso remoto que permite la gestión de los archivos y la ejecución de comandos.

Puerto 2155, 5512
El daemon Illusion Mailer es un programa de spamming de correo electrónico que permite enviar mensajes aprovechando la identidad de la víctima.

Puerto 2565
El servicio Striker, asociado a este puerto, tiene como único objetivo echar a Windows. Después de reiniciar ya no reside en la memoria y si se evita el ataque no se corren riesgos posteriores.

Puerto 2583, 3024, 4092, 5742
Un caballo de Troya conocido con el nombre de WinCrash, saca partido a estos puertos para introducirse y cumplir su acción. Como está dotado de instrumentos como el flooding, es considerado un instrumento potente y peligroso.

Puerto 2600
El daemon RootBeer es un caballo de Troya dotado de acceso remoto con las siguientes características: mensajería, control de ventanas, control del monitor, control de audio, control del módem, congelación del sistema.

Puerto 2989
El servicio RAT es un caballo de Troya con backdoor proyectado para destruir el contenido de los discos duros del sistema.

Puerto 3459, 3801
El daemon Eclipse es un servicio FTP invisible que da acceso a la transferencia de archivos y a su ejecución, eliminación y modificación.

Puerto 4567
El servicio File Nail es un backdoor remoto asociado al ICQ.

Puerto 5001, 30303, 50505
El virus Sockets de Troie es un programa que se difunde como backdoor de administración remota. Su instalación coincide con un error de instalación DLL y, después de instalarse en el directorio \windows\system, modifica las claves del registro de configuración.

Puerto 6400
El daemon tHing tiene su peligrosidad no tanto en su actividad intrínseca, sino porque es explotado por virus como método de infección de otros PC.

Puerto 7000
El daemon Remote Grab puede hacer capturas de pantalla del monitor remoto, de modo que da una visión exacta de la actividad desarrollada.

Puerto 10101
El caballo de Troya BrianSpy está dotado de todas las funciones clásicas de estos programas, además de un servicio gracias al que consigue eliminar los archivos de escaneo de los antivirus instalados.

Puerto 12223
El servicio que utiliza este puerto es un KeyLogger que tiene la posibilidad de enviar en tiempo real al cracker toda la actividad desarrollada en el teclado del ordenador remoto.

Puerto 12345
Quizá el más conocido de los puertos desconocidos: es el puerto al que responde el servidor del backdoor NetBus, ya viejo pero aún capaz de hacer daño.

Puerto 20000
El troyano Millenium es un programa escrito en VB que ofrece como características: control de archivos, control de CD-ROM, control de la barra de aplicaciones, control de audio, sustracción de password, control de browser, reinicio del sistema.

Puerto 22222, 33333
El caballo de Troya Prosiak es el enésimo daemon de control remoto que ofrece el clásico arsenal de funciones típicas de esta categoría de programas.

Puerto 31337, 54320
El daemon Back Orifice es un programa altamente peligroso que está en la base de la concepción de desarrollo de otros troyanos para Windows.

Prudencia ante todo

Como es fácil imaginar, la posibilidad por parte de un cracker de tener libre acceso a los puertos es de vital importancia para cumplir su obra destructiva. Esta larguísima lista de puertos y servicios asociados debe servir como estímulo para la autoprotección. Un buen cortafuegos, aunque no sea la solución a todos los males configurado en los límites de lo posible con reglas bastante férreas sobre la posibilidad de usar determinados puertos, puede ciertamente limitar los puertos de entrada al PC por parte de extraños. Si a esto asociamos también un escaneo periódico con antivirus y un escaneo del propio sistema a la caza de "puertos abiertos" probablemente conseguiremos tener una fotografía suficientemente exhaustiva de nuestra seguridad, entrando así en la posibilidad de correr a reparar cerrando los distintos fallos de nuestro PC.

CÓMO BORRAR (DE VERDAD) ARCHIVOS RESERVADOS O "COMPROMETEDORES"

A VECES VUELVEN



Incluso si has borrado un documento y vaciado la papelera de reciclaje, el contenido puede ser fácilmente recuperable con poco esfuerzo.

¿Estás seguro de haber realmente borrado los datos del disco, o sólo los has "escondido bajo la alfombra?"

Es bastante evidente que en los modernos sistemas operativos con interfaz gráfica, después de haber trasladado un archivo a la papelera, ésta no se borra sino que sigue accesible hasta que se efectúa el vaciado de la papelera. Lo que la mayoría de las personas no saben es que **el archivo puede ser fácilmente recuperado incluso después de vaciar la papelera**, y que por tanto cualquier usuario apenas experto y bastante motivado puede recuperar cualquier documento. Y apropiarse de la información que contiene en su interior, una vez recuperado.

>> Nada anormal

Esto no suena extraño ni singular a quien sepa cómo funciona el sistema de archivos de un ordenador. Cuando se guarda un documento en el disco duro, los datos se graban como una secuencia de ceros y unos en una determinada posición del disco; para saber dónde recuperara un determinado documento, el sistema debe tener un "registro" en el que señala la posición de todos los archivos. **Cuando se borra un archivo** con las funciones normales del sistema operativo, se "marca" como borrado y se eliminan las referencias, pero **los datos propiamente ni siquiera se tocan**. Comparando con el mundo físico, suponiendo que se quiere tirar un libro contenido en una biblioteca el sistema operativo no haría otra cosa eliminar la tarjeta del libro del índice de las obras y pegar una etiqueta de "eliminado" sobre la cubierta del libro. El libro permanecería en su posición hasta el momento en que hará falta espacio para insertar otro libro (o sea, registrar otro archivo). Sólo cuando será necesario registrar encima de la misma porción de disco, los datos se eliminarán (incluso en este caso es

> ? **Formateo** a bajo nivel: Un proceso análogo al simple formateo de un disco, pero que proporciona la puesta a cero de todos los bits.





posible recuperar los datos escritos precedentemente, pero en este punto llegamos a soluciones de fantaciencia, que requieren mucho tiempo y aparatos especiales). En resumen, si no se "adjuntan otros libros", bastaría con pasar revista de las estanterías para encontrar (¡y leer!) todos los discos erróneamente considerados eliminados. Y esto es más o menos lo que hacen los programas como Norton UnErase o R-Undelete de R-Tools Technology.
Si crees que puedes estar tranquilo, porque has formateado el disco, haremos que te preocupes rápidamente: cuando se formatea el disco con las varias "modalidades rápidas", no se hace otra cosa que tirar el "registro" de archivos (la File Allocation Table); **una vez más, los archivos se quedan donde siempre han estado: en el disco.**

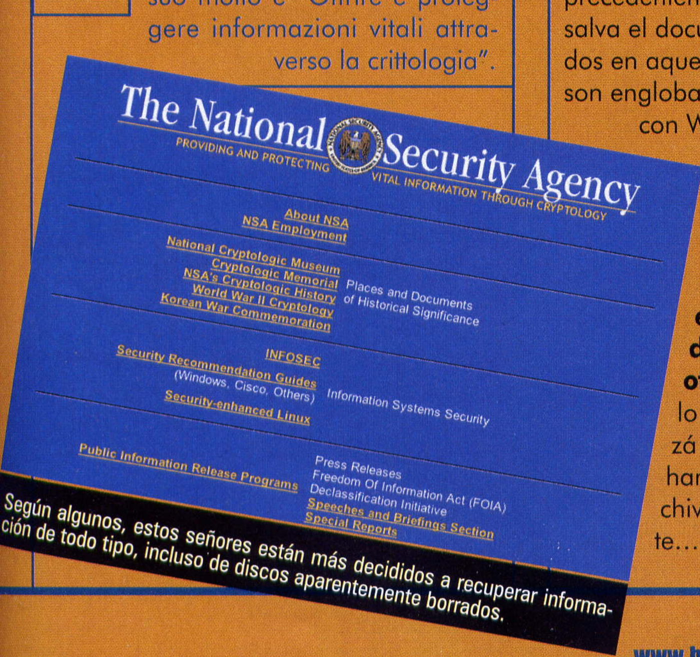
>> Situaciones de pánico

Alguien estará ya temblando pensando en el hecho de que todas las imágenes de las señoritas simpáticas y desinhibidas que ha borrado de su ordenador pueden ser fácilmente recuperadas por una madre o una novia un poco manitas. Pero esta es una de las situaciones menos graves. **Intenta pensar qué puede pasar después de vender el ordenador a un desconocido** o, (como pasa a menudo) cuando el viejo ordenador de un dirigente de una empresa es pasado a un asistente (quizá frustrado por el hecho de que el jefe tiene ordenador nuevo y, como de costumbre, a él le tocan las sobras...). **Información y comunicaciones reservadas, códigos de acceso a bancos de datos o cuentas corrientes, acuerdos estratégicos... todo en las manos del primero que pasa.**

UN FAMILIAR O UN AMIGO CURIOSO PODRÍAN CON POCO ESFUERZO LEER LOS ARCHIVOS QUE CREÍAS HABER BORRADO DE TU ORDENADOR.

Pero hay cosas peores: a causa de un bug de ciertas versiones de Office, podrías encontrarte enviando documentos que contienen porciones de archivos borrados. Cuando Word crea un nuevo documento, reserva cierto espacio en el disco, en el que se memorizan junto a la información necesaria para la apertura del documento (fuente, estilo, lengua, etc.) todas las versiones precedentes y la información necesaria para recuperar un documento en caso de bloqueo del ordenador. Como decíamos el espacio es "reservado" por el documento de Word en el acto de su creación: volviendo a nuestro ejemplo, Word se "toma para él" un par de estanterías de la librería, pero sin vaciarlas de los libros precedentemente borrados. Cuando se salva el documento, los datos contenidos en aquella porción de disco duro son englobados: abriendo el documento con Word, no se notará nada distinto (porque estos datos no forman parte del documento), pero **si se abre el archivo .doc con un editor de puro texto o con un editor hexadecimal, se podrán leer fragmentos de otros documentos.** Si no te lo crees, haz una prueba, quizá utilizando un disco del que han sido borrados muchos archivos de texto: es escalofriante...

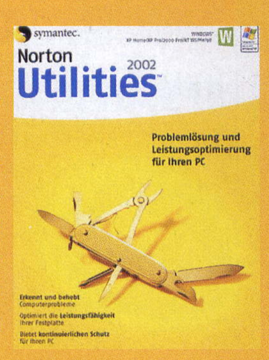
? **NSA National Security Agency.** L'agenzia per la sicurezza nazionale americana. Il suo motto è "Offrire e proteggere informazioni vitali attraverso la crittologia".



Según algunos, estos señores están más decididos a recuperar información de todo tipo, incluso de discos aparentemente borrados.

PROGRAMAS PARA RESUCITAR UN ARCHIVO...

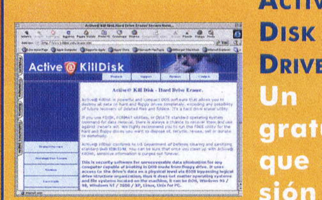
NORTON UTILITIES
En el popular paquete de utilidades, el programa UnErase permite recuperar archivos borrados, incluso iniciando desde DOS (cosa aconsejable).



DISK INVESTIGATOR
Un programa que lee los datos sucios directamente del disco duro, bypasando la información proporcionada por el sistema. Es gratuito y se descarga en www.theabsolute.net/sware/dskinv.html

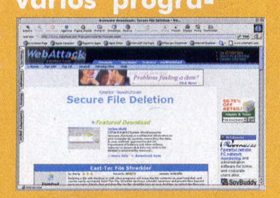
...Y PARA ELIMINARLO DE VERDAD

PGP DISK
La funcionalidad Document Wipe de PGP permite sobrescribir archivos con datos casuales en varias pasadas, a elección del usuario.



ACTIVE@ KILL DISK - HARD DRIVE ERASER
Un software gratuito pero que en su versión de pago está conforme a las directivas para la "limpieza y desinfección de datos" del Departamento de Defensa americano. Se descarga de www.killdisk.com/eraser.htm

VARIOS FREEWARE
En la dirección www.webattack.com/freeware/security/fwerase.shtml hay una lista de varios programas gratuitos para el borrado seguro de archivos.



CÓMO BORRAR (DE VERDAD) ARCHIVOS RESERVADOS O "COMPROMETEDORES"

CON MICROSCOPIOS DE FUERZA MAGNÉTICA SE PUEDEN LEER INCLUSO LOS DATOS BORRADOS Y SOBRESCRITOS

>> Cómo hacer borrón y cuenta nueva

Para estar seguro de haber borrado de verdad un documento, hace falta usar un programa que escriba **una secuencia de datos binarios casuales distinta** en la misma porción de disco en la que se encuentra el archivo que eliminar. Existen varios programas de este tipo, y la función de "borrado seguro" se incluye en varias suites de utilidades (como las famosas Norton de Symantec) o en programas de privacidad y criptografía (tipo PGP). Algunos programas se limitan a borrar en modo seguro un documento aún perfectamente visible: se selecciona el archivo deseado y será borrado en modo seguro e irrevocable (ojo

>> La paranoia nunca es exagerada

antes de borrar documentos que podrían ser aún necesarios...). **Otros programas, en cambio, trabajan sobre los archivos que ya han sido borrados, haciendo una función de "relimpieza"** de todas las áreas del disco que han sido marcadas como "área libre" para la escritura de nuevos archivos, pero que -como hemos visto- podrían contener datos. Las dos funciones son útiles y la mayor parte de los programas de "borrado seguro" pueden hacer ambas funciones.

Antes decíamos que los programas de borrado seguro no se limitan a poner a cero (o uno) los bits del área ocupada por el archivo, sino que escriben en el disco "una secuencia de datos binarios casuales distinta". Esta diferencia puede ser considerada una sutilidad irrelevante para la mayor parte de los usuarios (que quieren proteger la propia privacidad de colegas o familiares curiosos), pero para algunos asume una importancia... vital.

Incluso si están sobrescritos y no recuperables de los cabezales del disco duro, los datos borrados dejan en la superficie del disco **una "huella" magnética muy débil pero identificable con los instrumentos adecuados**, como un aparato para Microscopia de Fuerza Magnética (MFM). Con el instrumento adecuado (algunos modelos de microscopios MFM ya están equipado para analizar superficies de disco duro...), **una persona preparada podría "ver" los bits borrados con la misma facilidad con que un texto a lápiz borrado con una goma puede ser leído poniendo la hoja de papel a contraluz.**

Escribiendo una secuencia únicamente de "ceros" o "unos" en el disco, la información puede ser recuperada en base a la diferencia de fuerza magnética que existe entre los bits que antes del borrado contenían un cero y los que antes contenían un uno. Volviendo a nuestro papel con el texto borrado, es un poco como aplicar encima una hoja de papel de copiar: a contraluz el texto se ve igualmente. Justo por esto los programas "serios" sobrescriben los datos con **una secuencia casual de datos y no se limitan a una simple reescritura, sino que ejecutan varias pasadas.** (en algunos casos el número es a discreción del usuario). En general, **tres pasadas son consideradas un razonable compromiso entre seguridad y práctica**: el tiempo de borrado aumenta de manera proporcional al número de pasadas.

Algunos objetan que la recuperación de información de porciones de disco sobrescritas con otros datos **son cosas que se ven solamente en películas de espionaje**. Será así, pero el NSA parece tomar en serio la cuestión, y el Departamento de Defensa americano ha realizado una directiva para a eliminación segura de datos. **Si se preocupan ellos, ¿por qué no debemos hacerlo también nosotros?**

Rimanendo in attesa di un cortese riscontro da parte Vostra,
porgo i miei più Codiali Saluti.

Pinco pallino

□□□F□g□h□k□{□ê□π□Œ□œ□.□□□□□,□90:□;□□□z□{□}□í□ì□∞□±□›□ﬁ□‡□□□□□□□
2□ÒÁ›Œ›ƒ›ª›ª±ª©›°öêöàêàö›±z±iz±XzS0J□mH□□!□Å□j□□□5Å6Å0J□QJ□
U□mH□□!□Å□jZ□□5Å6Å0J□QJ□U□mH□□□□j5Å6Å0J□QJ□U□mH□□□6ÅCJ□0J□QJ□
□0J□QJ□hmH □nH □□CJ□0J□QJ□□5Å6Å0J□QJ□□5Å0J□QJ□mH□□□5Å6Å0J□QJ□
mH□ BANCOMAT:□34556 CJ□0J□QJ□mH□□□□j6ÅCJ□0J□QJ□U□mH□□ □
QJ□U□mH□□□5ÅCJ□0J□QJ□mH□□□6ÅCJ□0J□QJ□mH□□□□j>□5ÅCJ□0J□
Cara Caterina,□purtroppo non possiamo vederci spesso quanto vorrei.□ Se mia moglie scoprisse della nostra relazione sarebbe una tragedia
□□"□F□G□H□f□g□i□j□k□}□~□□□ƒ□ª□°□Œ□œ□□□□□□□+□,□í□ì□
ı••••Î•Ê□
5□,.....
&□F□□
&□FÔ□
&□□F□
&□F•□□□$□□□□□"□F□G□H□f□g□i□j□k□}□~□□□ƒ□ª□°□Œ□œ□□□□□□□+□,□í□ì□5□
&□F•□□□$□□□□□"□F□G□H□f□g□i□j□k□}□~□□□ƒ□ª□°□Œ□œ□□□□□□□+□,□í□ì□5□
6□é□è□ê□¿□¡□¬□«□»□◊□ÿ□Ï□Ì□Ó□¯□□□S□T□_□z□¨□ﬁ□□□□'I£≈Ÿ.·····ÙÓ
ÎÎÎÎÎÎÈÎ‰‹ÈÎ'Ãƒ°¥ÈÎ¨§úî□□□□
Ë □

Esta imagen ha sido recreada artificialmente para demostrar qué podría revelar un documento de Word que haya incluido fragmentos de información casuales tomados de la memoria y del disco. Los programas que sufren este problema son Microsoft Word 6.0 y 7.0 y la versión 7.0 de Power Point y Excel. Microsoft ha lanzado actualizaciones que lo corrigen.

40 µm, MFM images of a zip disk

60 | 0 au | amplitude | 700 | 0 au | phase

La superficie magnética de un disco Zip analizada con un microscopio de fuerza magnética.

PARA SABER MÁS...

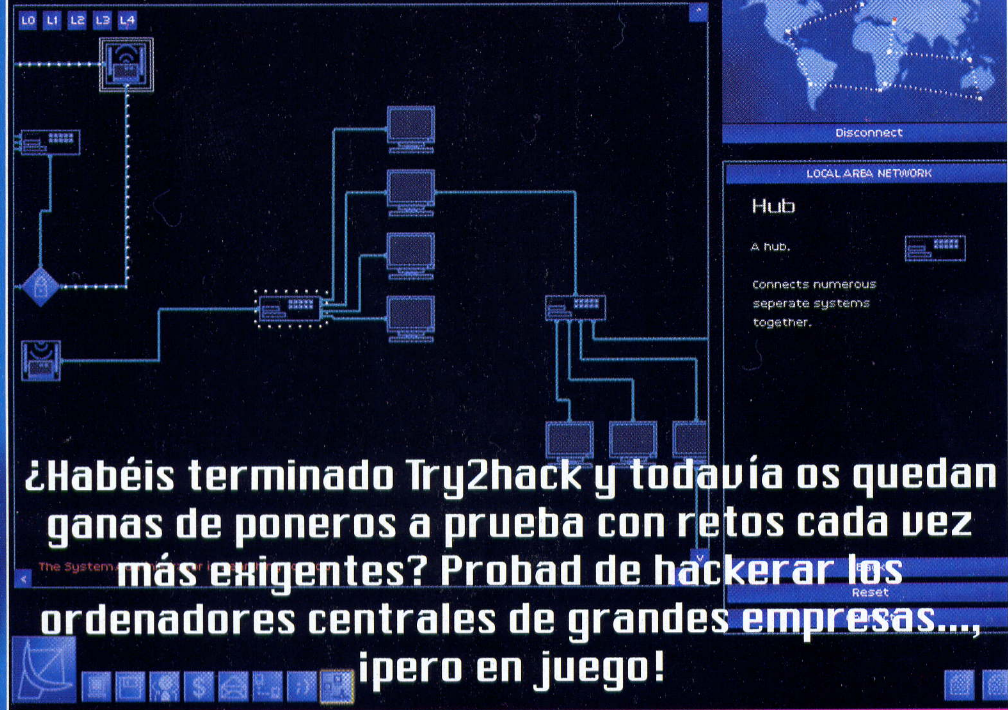
www.cs.auckland.ac.nz/~pgut001/pubs/secure_del.html
Una auténtica Biblia sobre los aspectos más científicos de la lectura de información de los soportes magnéticos.

ftp://ftp.cerias.purdue.edu/pub/lists/best-of-security/326
Patente de la NSA para la recuperación de campos magnéticos en soportes sobrescritos.

www.all.net/books/standards/remnants
Guía para la comprensión de datos residuales en los sistemas informáticos de Computer Security Center.

Uplink

El simulador de hacking



¿Habéis terminado Try2hack y todavía os quedan ganas de poneros a prueba con retos cada vez más exigentes? Probad de hackerar los ordenadores centrales de grandes empresas..., ¡pero en juego!

CUANDO EL HACKING SE CONVIERTE EN VIDEOJUEGO

Después de esta obligada introducción, pasamos a la descripción de este revolucionario simulador de Introversión. Se tendría que premiar a los creadores de este título por su originalidad y por haber tenido las agallas de ir contra tendencias (que es la filosofía que hay detrás del juego en cuestión). Y es que los desarrolladores, un grupo de jóvenes estudiantes de ingeniería de Londres, han **dejado de lado el aspecto gráfico para centrarse en una buena programación** (ya estamos hartos de productos gráficamente superlativos, pero llenos de bugs).

¿Pero, de qué se trata? Uplink se encuentra en la categoría de los "simuladores" y para jugar os **tendréis que poner en la piel de un joven hacker principiante**, miembro de la asociación Uplink. El juego se ambienta en un hipotético 2010 y **la interfaz grafica recrea una pasarela, caracterizada con máquinas sofisticadas y componentes de hardware estremecedores**. Las músicas recrean perfectamente la atmósfera y en ciertos instantes se hace persecutoria, haciendo aumentar la adrenalina ¡al máximo!

>> De newbie a guru

Lógicamente empezaréis con un ordenador y un módem, pero superando las diferentes misiones que se os propondrán, se os compensará con dinero, que os servirá para aumentar las capacidades del ordenador y poder hacer así trabajillos cada vez más sofisticados... Entre los componentes de hardware que tendréis que instalar están el módem, la CPU, la memoria RAM, los sistemas de monitorización y otros. Y no se termina aquí, podréis, o mejor dicho, deberéis, si queréis subir de nivel, **comprar software, desde programas levantadores de password hasta sofisticados programas de cifrado**.

Aun siendo un juego totalmente offline, el nuevo patch que han lanzado los desarrolladores añade, entre los programas que se pueden comprar, un cliente irc para poder chatear en el interior del juego. Y quizás poder desafiar en tiempo real a otro hacker de verdad... ¡Como veis, "el juego resulta duro"!

>> Empezar a jugar

Antes de acceder al juego os tendréis que registrar como agente, insertando vuestro nick y un password. Después de ello, tendréis que elegir la configuración de vuestra pasarela y el juego estará a punto. Os encontraréis delante de un escritorio y recibiréis inmediatamente un correo electrónico que os presentará el que será vuestro próximo trabajo. Pero antes de ponerse a "trabajar" Uplink os quiere poner a prueba. En otro mail os **invitará a entrar desde remoto en un sistema protegido por password y robar un determinado archivo**. Una vez hecho esto, salvad el archivo en vuestra memoria y mandad un correo a la empresa que se ha puesto en contacto con vosotros, adjuntando el archivo en cuestión... Y ya está, a partir de este momento tendréis acceso a una serie de misiones, obviamente según vuestro grado de preparación las misiones que se os propondrán serán cada vez más difíciles, y obviamente mejor recompensadas ;).

Uplink existe para Windows y Linux y cuesta 33,99 Euros. Desde el sitio del productor, www.introversion.co.uk, puedes descargar una versión demo.

IMPLEMENTACIÓN DE UN CORTAFUEGOS EN LINUX CON IPTABLES

ALEJANDO A LOS INTRUSOS

En la mayor parte de las instalaciones Linux está ya presente la función de cortafuegos. Descubre con nosotros cómo se puede configurar el sistema para rechazar los paquetes desagradables.



Linux contiene el soporte para enrutamiento y filtro de los paquetes de red, que se usan mediante IpTables e IP Chains. IP Chains es más viejo con respecto a IpTables: si tienes un kernel anterior al 2.2, estarás obligado a usar Ip Chains; si en cambio tienes alguna distribución superior (la 2.4 es la versión más estable), IpTables es la elección adecuada. Este último software soporta mejor el enmascaramiento y los filtros de paquete (de la 2.3, NetFilter).

Los paquetes que atravesarán el cortafuegos serán confrontados con las tablas de IpTable; si un paquete corresponde a ciertas reglas (llamadas también ACL, de Access Control List), el paquete se elaborará en consecuencia.

Para la máxima protección, se aconseja también instalar un sistema de identificación de las intrusiones (IDS, del que hablaremos en seguida). Linux permite enviar

>> Configuración del cortafuegos como filtro

paquetes Ip, cosa que permite configurarlo como enrutador. Si tienes un ordenador con una dirección de red interna, este ordenador no podrá salir a Internet porque tendrá una IP reservada a las redes locales. Los paquetes entran por una tarjeta Ethernet y son traducidos e introducidos en Internet con la IP del enrutador o del cortafuegos conectado a Internet. Este tipo de cortafuegos se llama server proxy. Además es posible enviar o modificar encabezamientos IP mediante IpTables, para que alcancen la red de Internet.

Para esto IpTables manda los paquetes al kernel para elaborarlos. El enmascaramiento usa el servicio NAT que permite usar una dirección de IP para más de un sistema. Este servicio, basado en Upchains, no es compatible con los clientes VPN que usan PPTP.

Crear una tabla con todas las reglas puede ser un rompecabezas, sobretodo si se usan redes muy extensas. Para esto, con IpTables, a veces basta con asignar reglas predefinidas y modificarlas al gusto.

Para crear un filtro a los paquetes de salida (procedentes del interior), es aconsejable negar todos los accesos y seguidamente aceptar los que sirven a un determinado servicio. Por ejemplo, si A (ordenador interno) debe acceder a un servicio http en un servidor Web de la otra parte del ordenador B (cortafuegos) el ordenador B deberá dejar abiertos los puertos 80 y 443 (para el http).

Para crear las reglas para los paquetes de entrada es aconsejable bloquear todo el tráfico ICMP con el fin de evitar los ataques DoS, pero esto podría complicar la resolución de los problemas en una red muy amplia.

Haría falta también bloquear todo el tráfico de entrada a menos que no forme parte de una conexión ya abierta.

En Ip Chains se usa la opción -y y -SYN de modo que el cortafuegos rechace los paquetes con el flan SYN configurado, y en cambio los paquetes con el bit FIN o ACK son aceptados porque forman parte de una sesión ya abierta.

Otra cosa muy importante es habilitar el registro de los paquetes. Con Ip Chains se usa el parámetro -l, com IpTables -j LOG (destino).

Para poder sacar partido del cortafuegos con plenas prestaciones es necesario configurar las opciones Network Packet Filtering en la




sección NEtWorking en los kernels hasta la 2.2. En las versiones posteriores, en cambio, deberían haber las opciones: Network Cortafuegos, TCP/IP networking e IP accounting.
Esta última opción (IP accounting) es necesaria para recoger los datos sobre los paquetes y permite obtener información sobre el uso

¿Cómo se instala?

Los paquetes IPchains e IpTables a menudo los montan las distribuciones más difundidas en el momento de la instalación de Linux. Si no fuera a sí probablemente deberás recompilar el kernel para incluir estas opciones.

de la red. Para esto el siguiente archivo debe estar en el directorio /proa/proa/net/ip_acct. Si el archivo existe quiere decir que el kernel soporta ya la función para el filtro de paquetes.

Pasemos ahora a las tablas y a las cadenas. IpTables usa tablas predefinidas que interactúan con las interfaces del sistema y gestionan los paquetes como consecuencia.
Las cadenas son reglas que usa IpTables. Como se puede ver en el recuadro "Las tablas de IpTables", este programa usa tres tablas: NAT, Mangle y Filter. IpTables usa la tabla Filter para filtrar los paquetes y la tabla NAT para enmascararlos (pero si no está especificada IpTables usa Filter como predefinida).

En la tabla Filter hay tres cadenas predefinidas:
INPUT: contiene las reglas para los paquetes de entrada;
FORWARD: contiene las reglas que dirán si el paquete necesita una máscara;
OUTPUT: contiene las reglas para los paquetes de salida.
En las tablas NAT y Mangle hay dos tipos de cadenas diferentes respecto a Filter:
PREROUTING: modifica los paquetes que intentan entrar en la interfaz;
POSTROUING: modifica los paquetes cuando dejan el host (de salida).
Pasemos a la parte práctica. Para

>> Acciones de las cadenas y programación de las reglas

establecer qué reglas aplicar, naturalmente se debe primero delinear un perfil de la red, y esta es quizá la parte más complicada. Los comandos son simples y sobretodo pocos, pero la cosa más difícil es saber exactamente qué finalidad tiene cada paquete, con el objetivo de evitar desagradables errores al programar las reglas que provocan las intrusiones informáticas. las opciones más usadas son DROP y ACCEPT

gos pueden haber diversas tarjetas de red: por ejemplo, una para la red interna y otra para la red externa. Si no se especifica una interfaz de red se usará la primera (por ejemplo eth0).
En un sistema con dos tarjetas esta opción es necesaria porque en una red se puede querer bloquear todo el tráfico TCP de entrada de la red pero aceptarlo de salida. Para tal cosa se usa la opción -i para especificar la interfaz:

```
iptables -A INPUT - i eth0 -s 0/0 -d 0/0 -protocl icmp-type echoreply -j REJECT
iptables -A INPUT - i eth1 -s 0/0 -d 0/0 -protocl icmp-type echoreply -j REJECT
```

Este comando permite todo el tráfico ICMP en una red, pero no los envía con un paquete echoreply (adiós ping).
Otra cosa importante: las políticas están configuradas por defecto en Accept, pero sería preferible antes

Tabla	Cadenas Predefinidas	Descripción
filter	INPUT FORWARD	Filtra los paquetes
Nat	PREROUTING OUTPUT POSTROUTING	Permite la máscara
Mangle	PREROUTING OUTPUT POSTROUTIN	Altera los paquetes

Te conviene crear una cadena personalizada y modificarla a tu gusto, así:

```
iptables -N custom
iptables -A custom  -s 0/0 -d 0/0 -p icmp -j DROP
iptables -A input -s 0/0 -d 0/0 -j custom
```

En el ejemplo la opción A atañe una regla colocándola al inicio de la cadena; la opción -I atañe la regla al final de la cadena y seguidamente añade una regla que rechaza todos los paquetes ICMP de entrada.
(DROP = Respingere ACCEPT = Accettare)
Pero en el enrutador o cortafuegos

configurarlo todo en Drop y luego configurar sólo lo que se necesita en Accept. De esta manera se evitará dejar algún puerto abierto.

```
iptables -P input DROP
```

Para visualizar las reglas configuradas hasta ahora, puedes teclear lo que sigue:

```
iptables -L
```

Como IpTables tiene tres tablas puedes escoger visualizar sólo una con:

```
iptables -t nat -L
```

Si luego quieres visualizar sólo una cadena de una tabla, usa:



iptables -t nat -L FORWARD

Si quieres además salvar el resultado en un archivo (recomendable para resolver problemas) usa este comando:

/sbin/iptables-save > iptables.txt

(Atención: las versiones anteriores a la 1.2.1a no soportan esta opción)

Además, en el caso de que tu script personalizado a cada inicio del ordenador se active para configurar las reglas de cortafuegos puedes añadir la siguiente línea

iptables -F

que borra todas las reglas configuradas en Filter, pero no las de NAT o Mangle, que deben borrarse así:

iptables -t nat -F

>> Emmascaramiento en iptables

Para borrar sólo una cadena de Filter se usa el comando iptables -F pero con el nombre de la cadena (por ejemplo INPUT). Los servicios usados por Internet, como FTP, requieren un soporte añadido. IpTables proporciona varios módulos para el enmascaramiento, que permiten acceder a estos recursos: El comando para reclamar los módulos es el siguiente:

/sbin/insmod *nombremódulo*

Para enmascarar la Ip se usa el siguiente comando:

iptables -t nat -A POSTROUTING -d ! 192.168.1.0/22 -j MASCHERADE
iptables -t nat -A POSTROUTING -d ! 10.100.100.0/24 -j MASCHERADE

Esta regla se añade a la cadena postrouting (-A) de la tabla NAT (-t). Con el signo de exclamación se dice a IpTables que emmascare todos los paquetes no dirigidos a 192.168.1.0 puerto 22 y 10.100.100.0 puerto 24. Como configuración predefinida, IpTables usa la primera tarjeta de red. Para modificar esta elección, se usa la opción -o. Pero esta opción deja la red descubierta, porque si un cracker quiere entrar en el host de la red interna le bastará teclear la Ip del cortafuegos para obtener una conexión directa (las cosas son en realidad más complicadas). Para evitar esto, aplicamos la reglas de enmascaramiento sólo a la red interna:

iptables -A FORWARD -s 192.168.1.0/24 -j ACCEPT
iptables -A FORWARD -d 192.168.1.0/24 -j ACCEPT
iptables -A FORWARD -s 10.100.100.0/24 -j ACCEPT
iptables -A FORWARD -d 10.100.100.0/24 -j ACCEPT
iptables -A FORWARD -j DROP

Como decíamos al principio, con estos instrumentos es incluso posible registrar los paquetes rechazados, de manera que se tenga un log para examinar, a la búsqueda de huellas de un ataque o para resolver problemas en la red. En los próximos números veremos cómo se hace exactamente.

yhttp://accessdenied85.cjb.net

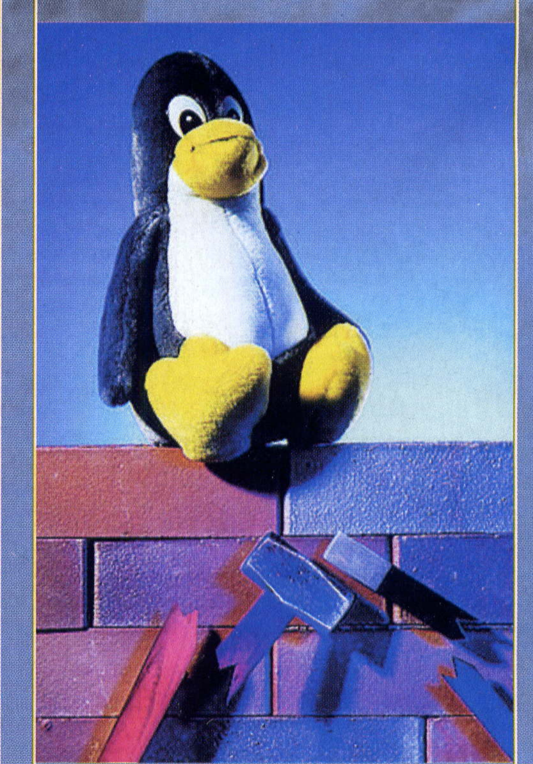
MÓDULO	DESCRIPCIÓN
ip_masq_ftp	Módulo para el enmascaramiento de las conexiones FTP
ip_masq_raudio	Para el real audio
ip_masq_irc	Para IRC
ip_masq_vdolive	Para las conexiones VDO Live
ip_masq_cuseeme	Para CU-See__Me

Mini cortafuegos

Si tu objetivo es proteger un ordenador directamente conectado a Internet mediante un módem casero (es decir, si no es la red de una empresa) puedes construirte un sencillísimo cortafuegos personal creando un banal script.
Por ejemplo, para bloquear el ping de tu ordenador y registrar los intentos de ping en un log bastará crear el siguiente script:

```
#!bin/sh
echo "1" >>
/proc/sys/net/ipv4/icmp_echo_ignore_all
exit 0
```

(para información posterior relativa a los scripts leed el tutorial en la dirección http://accessdenied85.cjb.net).

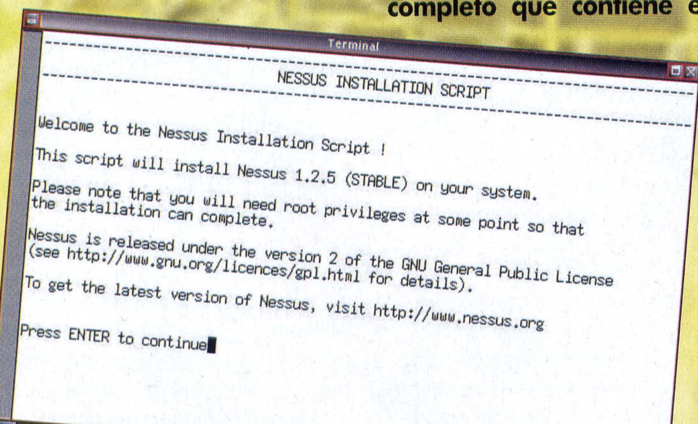


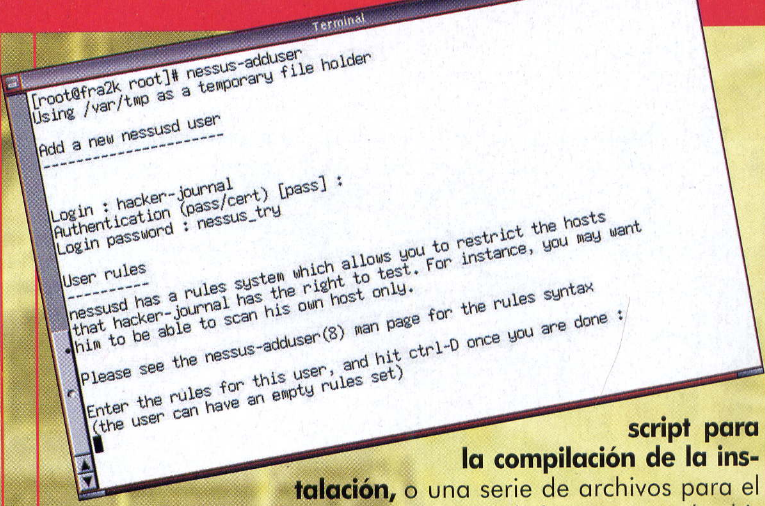
DEFENDERSE... ¡ATACANDO!

Nessus

A menudo nos preguntamos cuál puede ser el grado de seguridad de un sistema, por dónde se puede acceder a él o qué programas abren una puerta trasera o posibles DoS.

Nessus (www.nessus.org) es un escáner de seguridad completamente gratuito y constantemente puesto al día. Su función es la de **analizar sistemas o redes enteras para descubrir qué vías tienen los posibles crackers para colarse y causar daños**. El sistema de plug-in en el que se basa permite añadir fácilmente la posibilidad de reconocer los últimos gusanos descubiertos.
Nessus es un sistema remoto, **compuesto por una parte servidor y una cliente**. La primera es un demonio disponible sólo para los diferentes entornos Unix-like, como GNU/Linux, Bsd y Solaris. Es el corazón del escáner, en la medida que se ocupa de realizar los análisis y de simular los ataques. El cliente, en cambio, es sólo una interfaz gráfica para la configuración y gestión de Nessus, y está disponible tanto para entornos Unix como Windows.
Vamos a ver cómo se instala, configura y utiliza la versión Linux de Nessus para llevar a cabo un control del propio sistema. La primera operación que se tiene que realizar es evidentemente la de obtener los paquetes que contienen el programa. **Del sitio oficial se puede descargar un paquete completo que contiene el**





script para la compilación de la instalación, o una serie de archivos para el servidor, para los plug-ins, para el cliente y para las bibliotecas necesarias, todos para compilar a mano. Nosotros seguiremos la primera vía, sin duda más rápida y práctica para quien se aproxima a Nessus por primera vez.
Una vez puesto el installer en el directorio home, basta escribir (como usuario) el comando:

```
$ sh nessus-installer.sh
```

El script se ocupará de configurar el sistema, compilar los programas e instalarlo todo de la mejor manera. Para algunos de los procesos se pide una contraseña de usuario root, sin la cual no se puede llevar a cabo la instalación.

>> El server

La administración del servidor **la tiene que realizar necesariamente el usuario root**, puesto que tiene los máximos privi-

legios. Lo primero que hay que hacer es crear un certificado de conexiones Ssl. Con este fin se adjunta un script completamente automatizado: nessus-mkcert. Después, a través de la orden nessus-adduser es preciso insertar por lo menos un usuario que pueda conectarse al servidor para llevar a cabo los ataques.
Mediante el comando nessus-update-plugin **es posible además mantener al día la lista de plug-in disponibles**, para así buscar siempre todos los agujeros de seguridad disponibles en la biblioteca de escaneados de Nessus.
A partir de este momento, el servidor está correctamente configurado. Ya sólo falta lanzar el demonio escrito en este caso como usuario root:

```
# nessusd -D
```



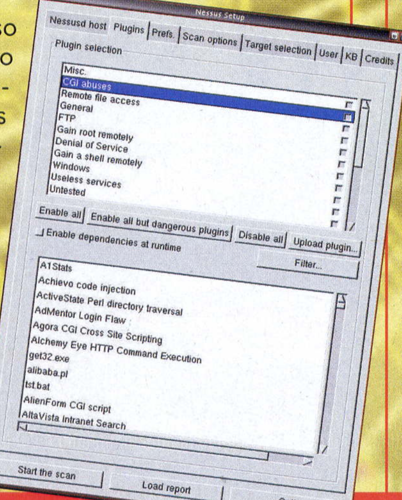
Plug-in: Los plug-in son módulos de Nessus que se ocupan de llevar a cabo los verdaderos ataques. Están escritos en NASL, acrónimo de Nessus Attack Scripting Language, un lenguaje de programación específicamente creado para escribir tests de seguridad para ser utilizados con Nessus.

>> Los clientes

Una vez configurado y puesto en marcha el server, **es posible conectarse desde qualquier host externo, si las reglas del cortafuegos lo permiten.**
La primera pantalla que aparece es la que se ocupa de pedir que se inserten los datos para la conexión y el login al servidor.

Una vez conectados, es preciso configurar el tipo de escaneado que se quiere efectuar. De entrada, es necesario seleccionar los plug-in que contienen las definiciones de los ataques que se quieren realizar.

La lista es muy larga y completa, y se enriquece de versión en versión. **Algunos de los plug-in pueden potencialmente colgar el sistema que se está probando**, así Nessus prefiere no habilitarlos por defecto,



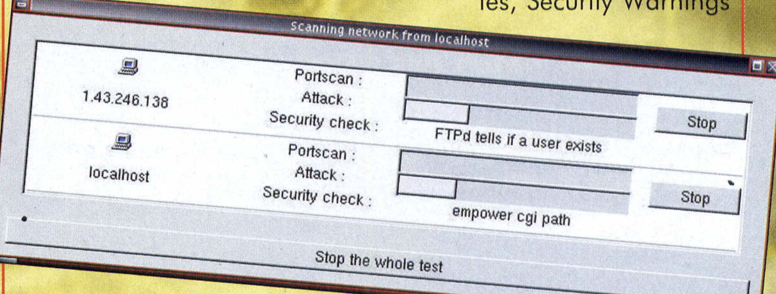
dejando activos sólo los que pueden ocasionar algún daño. De todos modos, es posible en cualquier momento activar también los módulos peligrosos, para llevar a cabo un escaneado más detallado.

Las opciones que se pueden configurar son muchísimas, pero para empezar podemos quedarnos con las que vienen por defecto. **La única opción importante de verdad es la elección del adversario**, en la pantalla Target selection. Si lo que queréis es probar vuestro propio ordenador, sólo tenéis que poner localhost, si no también se pueden escribir una serie de direcciones IP o nombres de dominio separados por una coma.
A partir de aquí todo está a punto, basta hacer clic sobre Start the scan para emprezar el test de seguridad.

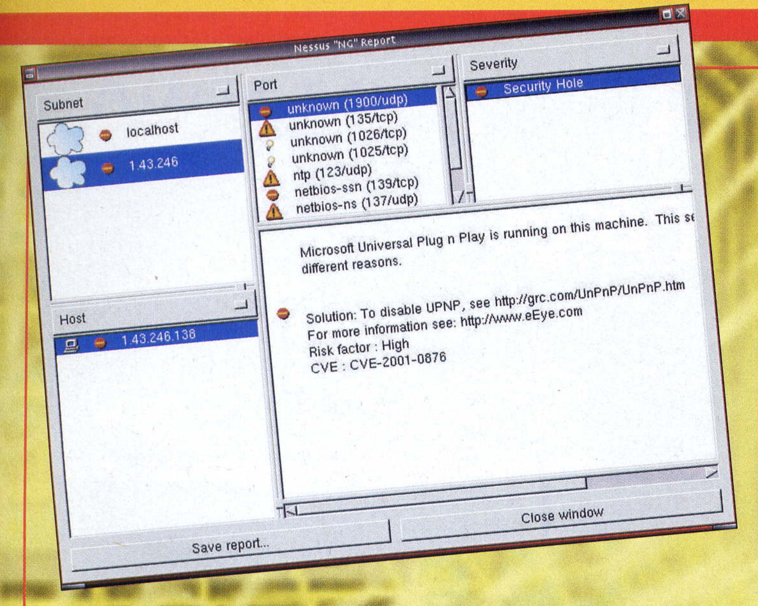
El test puede durar más o menos tiempo, dependiendo de la banda disponible, del número de hosts que se tienen que comprobar y de los plug-in activos.

>> El análisis de los resultados

Al finalizar esta operación, Nessus da los resultados de sus tests, subdivididos por sectores y host. El programa señala cuatro tipos de indicaciones: Serious, Security Holes, Security Warnings



y Security Notes.
Los agujeros de seguridad son los fallos a los que antes hay que poner remedio, sobre todo los que sean clasificados como Serious. A menudo son servidores con cuentas de default o protocolos bien conocidos como inseguros, todas ellas puertas abiertas hasta para los crackers más inexpertos. En la descripción del problema, **Nessus proporciona también posibles soluciones o direcciones web desde las cuales es posible descargarse los oportunos parches**.
En orden de importancia, siguen después las alertas. Estos son posibles problemas de seguridad, aunque de bajo riesgo. Queda pues a cargo de la experiencia de todo buen administrador de sistema decidir si seguir o no estas indicaciones, teniendo en cuenta que a menudo se indican también los servicios que se quiere que se vean desde fuera.
En resumen siguen algunas notas de seguridad, relativas sobre todo a la información sobre el sistema que un posible atacante puede conseguir. Son las versiones de los servidores, puertas abiertas, nombre de los hosts y otros detalles así. No comprometen directamente el sistema, pero ofrecen a los atacantes expertos instrumentos para estudiar un ataque eficaz.
El informe se puede salvar en varios formatos para permitir u-

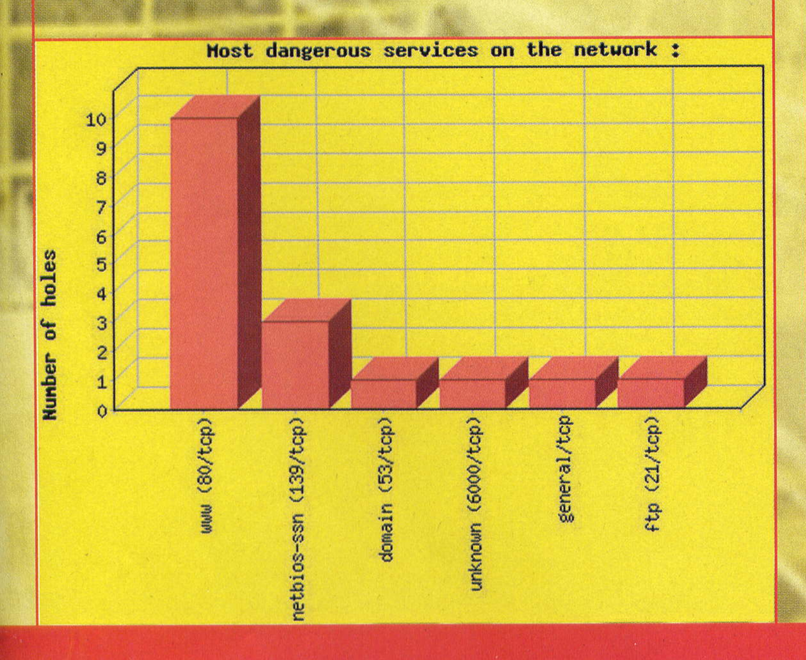


na consulta más en detalle. Entre las formas en las que se puede guardar está la posibilidad de **crear un informe detallado en versión Html**, con una serie de gráficos que ayudan a descubrir los problemas y los hosts más vulnerables.

>> ¡Utilizadlo correctamente!

Nessus es un sistema potente y versátil, pero hay que cogerle un poco de confianza para utilizarlo lo mejor posible. Por un lado, **permite reconocer todos los fallos de seguridad que hay en nuestro sistema**, sugiriendo las posibles correcciones. Por otro lado, permite encontrar los fallos y las puertas abiertas en sistemas remotos, aunque difícilmente pasará inadvertido un escaneado tan intrusivo como el que efectúa Nessus. En cualquiera de los casos, los resultados se tienen que interpretar correctamente, y **sólo la experiencia de cada usuario puede dar la clave de lectura correcta.**

Francisco "fra2k++" Facconi



Todos los plug in de Nessus

Actualmente para Nessus existen casi 1900 plug in, cada uno de ellos especializado en simular un determinado ataque. Muchos se incluyen en la distribución, pero otros más recientes se pueden descargar del sitio del programa (http://cgi.nessus.org/plugins). Se puede ver la lista completa, la que contiene únicamente los plug in lanzados después de la publicación de la última versión, o una lista estructurada por tipo de ataque. Las principales familias de plug in son:

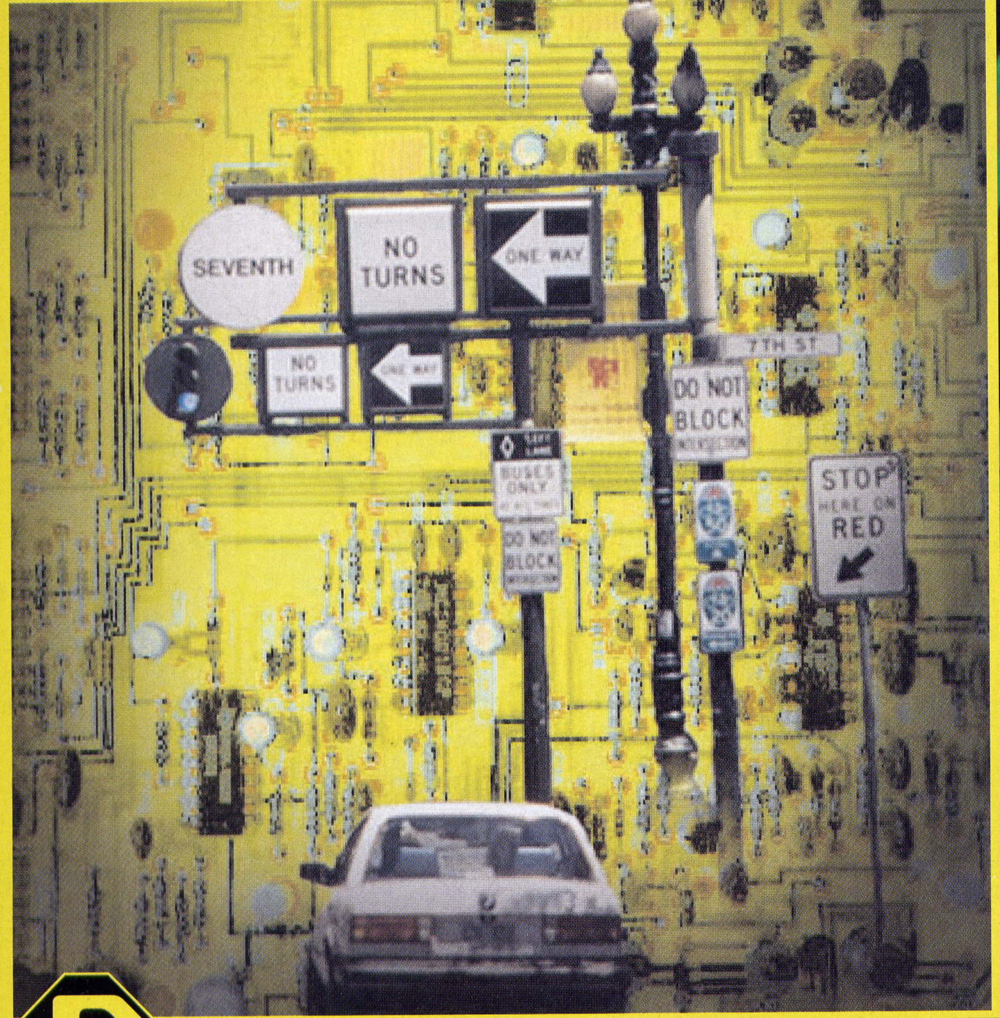
* Backdoor
* Abusos de los CGI
* CISCO
* Ataques Denial of Service
* Abusos di Finger
* Cortafuegos
* FTP
* Obtener una shell remota
* Obtener un acceso root desde remoto
* Netware
* NIS
* Port scanner
* Acceso remoto a los archivos
* RPC
* Disposiciones
* Problemas SMTP
* SNMP
* Servicios inútiles
* Windows
* Windows: gestión usuario

Es aconsejable tener instalados los plug in más recientes cuando se lleva a cabo un test, para permitir a Nessus reconocer los últimos fallos de seguridad descubiertos. La forma más simple de tener la lista al día es escribir en el shell del sistema en el cual está instalado el demonio y como usuario root, el comando nessus-update-plugins. Éste busca las actualizaciones, las descarga e instala correctamente en el sistema. Como alternativa es posible descargar del sitio de Nessus cada plug in, que es simplemente un script en leguaje NASL. Una vez obtenido el archivo, se copia en el directorio en el que están los plug in, que suele ser /usr/local/lib/nessus/plugins/. Y no olvidéis que es mejor reiniciar el demonio nessusd.

INSTRUCCIONES Y TRUCOS PARA ASPIRANTES A OPERADOR

IRC CREA Y GESTIONA TU CANAL

Gestionar un canal significa tener un gran poder sobre el resto de usuarios, pero, tal como debería ocurrir en el mundo real, el poder significa también responsabilidad.



Después del primer barniz que dimos en el pasado sobre lo que es IRC, su estructura y los primeros pasos a dar para entrar en este mundo, ahora entraremos más a fondo en el tema, estudiando cómo se puede abrir y gestionar un canal.
Partamos del supuesto de que en IRC existe casi todo, y que, por lo tanto, se pueden encontrar canales sobre cualquier tema del interés humano. Pero si queréis tener vuestro canal personal (o queréis simplemente haceros pasar las ganas), a continuación veremos cuáles son los procesos necesarios, los privilegios y los posibles problemas que podréis encontrar.

>> Los operadores

Un usuario cualquiera puede abrir un número ilimitado de canales simplemente ejecutando el comando en línea

`/join #miprimercanal`

Suponiendo que este canal no haya sido creado anteriormente tendréis una pantalla con vuestro único nombre arriba a la derecha precedido por una @. **Este símbolo os atribuye el estatus de operador del canal** con todos los privilegios y deberes que ello comporta.
La parte más delicada en cuanto a la gestión de un canal es la de decidir quién y qué admitir, el tipo de argumento a tratar (libre o limitado a un tema específico), los usuarios autorizados para acceder y todo aquello que tenga que ver con la gestión..
Los modos de canal son, por así decirlo, reglas que vosotros podéis determinar y que necesariamente se tienen que seguir. En general la sintaxis la da el comando

`/mode #canal +/-carta parámetro`

donde + indica la implementación y - la supresión del modo especificado.

>> Modos de un canal

Ahora veremos con detalle los tipos de canal, subdividiéndolos en aplicables al canal y aplicables a los usuarios.

Modo i (invite only): define la modalidad de invitación al canal. Sólo los usuarios que hayan sido invitados pueden acceder a él, al resto se le negará el permiso con un output del tipo "Can't access de chanel, invite only". Se aplica esta característica con el comando `/mode #canal +i`. Los usuarios pueden ser invitados del chan sólo por un usuario desde el interior del chan mismo con el comando `/invite nick #canal`





Modo l (limit): define el número máximo de usuarios que puede haber en el interior del canal. Así, quien intenta entrar una vez se ha alcanzado el número máximo determinado recibe un output del tipo "chan is full". Su sintaxis es `/mode #chan +l xx`, donde xx es el número límite establecido.

Modo n (no external messages): impide que los usuarios que no estén presentes en el interior del canal puedan enviar mensajes.

Modo k (key): define el password de acceso al mismo canal. Se determina con el comando `/mode #canal +k xxxxxx` donde xxxxxx donde xxxxxx es evidentemente la contraseña deseada. Un usuario que intente entrar en un canal +k recibirá un output del tipo "need correct key". Para entrar en un chan +k se tiene que utilizar el comando `/join #chan xxxxx`

Modo s (secret): configuración de canal que permite no dar información sobre dicho canal, no aparecer con el comando `/list` y tampoco en el `/whois` de un usuario a no ser que ambos estén en el interior del canal.

Modo t (topic): si se selecciona, este modo no permite a los usuarios -o cambiar el tema del canal.

Modo m (moderated): canal en modo m se define como "moderado" y sólo los +o o los usuarios con modalidad +v pueden interactuar en publico, mientras al resto les es prohibido. Quedan, por supuesto, activas para todos las query personales.

Modo p (privato): modalidad obsoleta, que ya no se utiliza y que no permite la visión del nombre del canal con un /list, pero que responde a la petición de otras informaciones.

```
] * sdsds (cat4r4tta@194.177.126.127) has joined #sdsds
] <CAT4R4TTA> sdsds is cat4r4tta@194.177.126.127 * model
] <CAT4R4TTA> sdsds on #sdsds
] <CAT4R4TTA> sdsds using *.tin.it [ircd.tin.it] - Telecom Italia Net - Italy
] <CAT4R4TTA> sdsds End of WHOIS list.
] * CAT4R4TTA sets mode: +b *!*@194.177.*
] * sdsds was kicked by CAT4R4TTA (CAT4R4TTA)
```

...n el ejemplo podéis ver el ban seleccionado por el usuario sdsds en el chan #sdsds (¡qué imaginación!) En la copia del /whois podéis ver la máscara y los datos necesarios para configurar el ban.

```
15:33] <[redacted]> Connected to [redacted], running eggdrop v1.6.10
15:33] <[redacted]> Eggdrop
15:33] <[redacted]> Hey CAT4R4TTA!  My name is [redacted] and I am running eggdrop v1.6.10, on FreeBSD 4.3-RELEASE-p29.
15:33] <[redacted]> Local time is now 05:30
15:33] <[redacted]> You are an owner of this bot. Only +n users can see this! For more info,
15:33] <[redacted]> see .help set motd. Please edit the motd file in your bot's 'text'
15:33] <[redacted]> directory.
15:33] <[redacted]> Use .help for basic help.
15:33] <[redacted]> Use .help <command> for help on a specific command.
15:33] <[redacted]> Use .help all to get a full command list.
15:33] <[redacted]> Use .help *somestring* to list any help texts containing "somestring".
15:33] <[redacted]> Have fun.
15:33] <[redacted]> Commands start with '.' (like '.quit' or '.help')
15:33] <[redacted]> Everything else goes out to the party line.
15:33] <[redacted]> [redacted] is running advanced [*war*] TCL version 4.6.6 by ^Boja^
15:33] <[redacted]> *------> Connected bots <------*
```

La party-line es el "lado-oscuro" del chat. Sólo aquellos que son "aptos" en los bot y su propietario pueden acceder a él. En este chat paralelo se ajustan las configuraciones de los bot y se instruye sobre los comportamientos que hay que tener.

>> Modos de usuarios

Modo o (operador): le da privilegios de operador al nick seleccionado. Los operadores tienen superpoderes, ya sea sobre los usuarios normales, ya sea sobre los otros operadores del canal. Se determina con `/mode #chan +o nick`.

Modo v (voice): el usuario que disfruta de este privilegio está autorizado a hablar en los canales +m. A menudo es inútil, porque los canales normalmente están en -m, pero aun y así se les da este privilegio a algunos usuarios como señal de simpatía hacia ellos.

Modo b (ban): permite determinar una prohibición de entrada a cualquier usuario que tenga una mascara igual al ban elegido. La identidad de cualquiera en IRC se da según el siguiente formato: nick|username@host.name, donde nick es el nick que se utiliza, username es el nombre del usuario y host.name es la dirección IP desde la que se conecta.
En la determinación de los ban existen caracteres especiales que se pueden utilizar. Son: (*) y (|). El primero identifica a cualquier grupo de caracteres incluido ninguno, mientras que el segundo indica cualquier carácter suelto pero no ninguno. Evidentemente estas prohibiciones pueden ser más o menos específicas. Si, por ejemplo, nos las tenemos que ver con un usuario indeseado que se conecta con una IP fija, poner un ban será muy fácil y no correremos el riesgo de incluir en la prohibición a otro usuario que no tenga culpa. Imaginemos que el usuario Ciao tenga una IP estática 111.222.121.212, introduciendo el ban

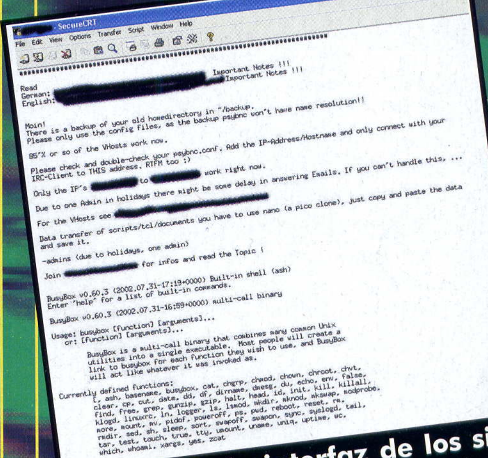
`/mode #chan +b hola!holamask@111.222.121.212`

tendremos la certeza de que el usuario no podrá entrar de nuevo en el canal, aunque podría cambiar de mascara, de ahí la necesidad de alargar el ban, que podría tomar la forma de

`/mode #chan +b *!*@111.222.121.212`

En el caso de un usuario con dialup e IP dinámicos el tema es más complejo, teniendo en cuenta que una vez desconectado y vuelto a conectar la IP cambia. Si se diese el caso que Hola tuviese como máscara

`hola!holamask@ppp-151.27.10.10.libre.es`



La shell es la interfaz de los sistemas Unix-like. En ella (entendida como cuenta en un servidor remoto) se encuentran los bot.

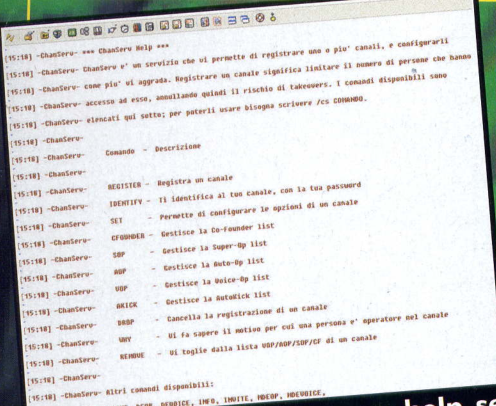
podríamos intentar poner un ban del tipo

`*!*holamask@ppp-*.libre.es`

con la esperanza que use siempre el mismo proveedor para conectarse. Tenemos que tener presente, de todos modos, que en este modo no ponemos un ban específico, por lo tanto, si hay otro usuario que utiliza libero.it y tienen como parte de su máscara "ciaomáscara" este se encontraría vetado en nuestro canal sin saber el porque. Se aconseja pues determinar bans lo más específicos posible, evitando dejar fuera a más usuarios de la cuenta. Es evidente







Con el comando /chanserv help se propone una ayuda on line con comandos principales, sus acciones y, si lo solicitáis, las cadenas de uso.

que si ponemos *!*@*.jp nadie se podrá conectar a nuestro chan desde un servidor japonés, tanto si son "buenos" como si son "malos".

>> La seguridad del canal

Si tenéis un canal, más tarde o más temprano empezaréis a pensar que un día u otro alguien querrá quitároslo. Hay varias maneras de hacerlo, pero las formas más utilizadas son sin duda los flood, los clones, y los collide.
Por flood se entiende el envío de una enorme cantidad de datos a un cliente o a un canal, una acción que a menudo lleva a la desconexión del cliente atacado y por lo tanto a la eliminación de las personas que están en el interior del canal. Los clones tienen el mismo principio de acción, basan su fuerza en su "replicación" con más clientes que tengan el mismo IP, y actúan con un ataque del tipo mircforce de flood. Los collide son técnicas más complejas, pero al mismo tiempo más eficaces y se basan en el hecho que en IRC no pueden haber dos usuarios con el mismo nickname. En caso de darse esta situación, se desconectan ambos clientes del servidor. La manera de llevar a cabo estas estrategias y su actuación práctica la trataremos más a fondo en el último de esta serie de artículos.

El ChanServ no está presente en todas las redes. En este ejemplo se ve el reconocimiento de un nick registrado por el usuario introduciendo el password.

>> Registrar un canal

En IRCnet no se prevé el registro de nicknames o de canales, pero en otras redes como Saura.net hay un servicio, el `chanserv`, que tiene esta función. Podéis descubrir fácilmente si existe y cómo se usa ChanServ con sólo escribir

```
/chanserv help
```

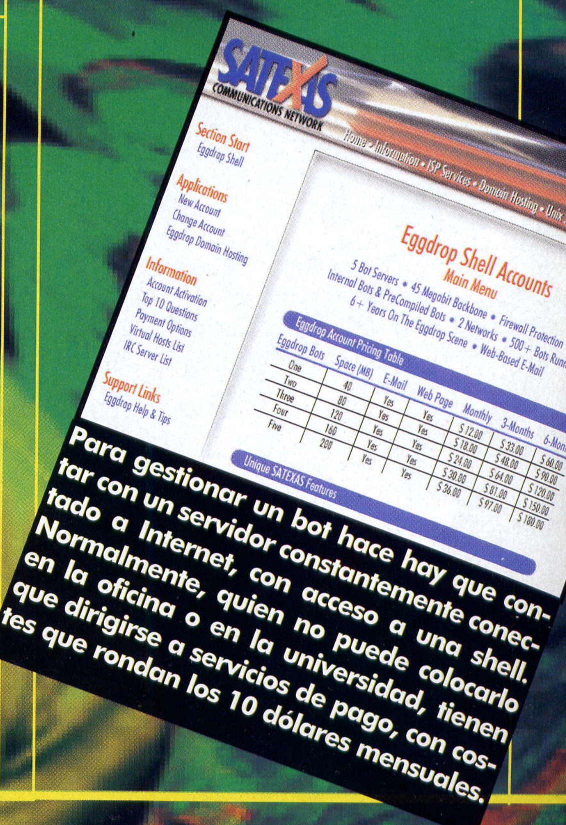
o bien

```
/msg chanserv help
```

Os aparecerá una lista de comandos y con cada uno de ellos podréis pedir un determinado tipo de ayuda.

>> BOT: el poder nocturno

¿Qué ocurre cuando es tarde y es hora de irse a dormir? Bien... si sois los últimos en salir de un cierto chan, el canal "se irá a dormir" con vosotros. En el momento en el que un canal queda vacío deja de existir y con él todas las configuraciones /mode efectuadas con tanto sudor de la frente. Para evitar esta situación se utilizan los bot. **Se trata de ciertos clientes que se sitúan en el shell remote, perennemente conectados a la red y totalmente gestionables en remoto.** Tienen estatus de operador del canal y están totalmente a vuestras órdenes, hacen todo lo que les pedís... y no ensucian :D
Pero, como en todas partes, también en los Bot no todo el monte es orégano. De entrada, tienen un coste. Bueno... ¿no estaréis pensando que alguien os deja tener un cliente en su propio servidor, con todo lo que ello puede comportar en ataques dDoS, gestión y gastos, sin haceros pagar un céntimo?!
Más allá del coste, la tocada de narices es la configuración. No se trata de nada especialmente complejo, pero siempre hay cosas que estudiar y practicar, porque al principio no hay nada de intuitivo. Considerando también el hecho que **normalmente se encuentran en plataformas linux/freeBSD y son gestionados por shell, con las cuales el usuario medio no se siente seguro, las cosas se complican un poco** para quien llega de Windows y con poca experiencia. Los Bot, como veremos detalladamente en el próximo número, seguro os ayudarán a gestionar vuestros canales, os ofrecerán una posición aventajada respecto al resto de usuarios, aunque no dejaran de ser máquinas "estúpidas" que si no están instruidas pueden crear problemas. En el artículo que encontraréis próximamente entraremos más en detalle en la programación de los Bot y hablaremos de las IRCwar, guerras a golpe de bit que tienen lugar en los canales IRC. Que os divirtáis en vuestros nuevos canales y, sobre todo, no olvidéis comentar a los amigos cuáles son.



Para gestionar un bot hace hay que contar con un servidor constantemente conectado a Internet, con acceso a una shell. Normalmente, quien no puede colocarlo en la oficina o en la universidad, tienen que dirigirse a servicios de pago, con costes que rondan los 10 dólares mensuales.

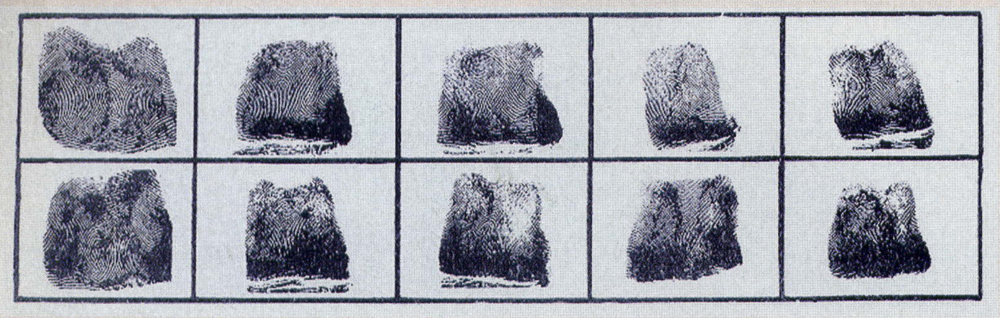
IDENTIFICATION ORDER NO. 10
October 10th, 2002

WANTED

DIVISION OF INVESTIGATION H.J. DEPARTMENT OF NET

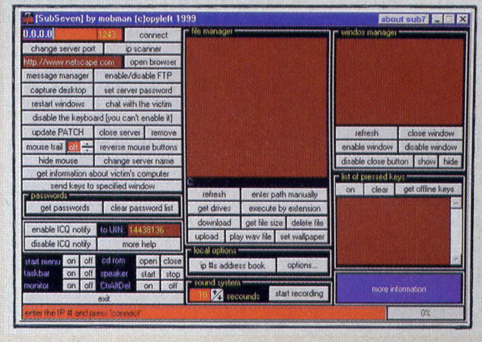
BARCELONA - ES.

NAME: NetBus
TYPE: Trojan
ALIAS: NetBus.153, NetBus.160, NetBus.170
DATE OF BIRTH: Marzo 1998
AUTOR: Carl-Fredrik Neikter



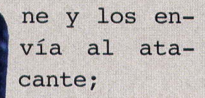
Fingerprint Classification

16 0 5 U 001 20
I 17 U 001



Acciones cumplidas:

Según las versiones, Subseven puede efectuar cerca de un centenar de acciones distintas; entre ellas, las más peligrosas son:
- registra sonidos desde el micrófono del ordenador atacado;
- captura imágenes desde una webcam eventual;
- lee los passwords del disco y de la memoria;
- registra las teclas presionadas por el usuario, incluso cuando está offline y los envía al atacante;
- notifica al atacante la presencia online de la víctima;
- captura la imagen de la pantalla;
- abre un servidor Ftp que permite al atacante descargar o borrar cualquier archivo de la víctima;
- modifica el registro de Windows;
- ejecuta aplicaciones;
- inserta comandos manuales;
- permite al atacante escribir en cualquier aplicación abierta.



Medios de contagio:

- Apertura de archivos ejecutables infectados recibidos vía email, a través de un chat Dcc en Irc o descargados de sitios no muy fiables (habitualmente, sitios "warez", "cracz" o porno);
- instalación directa por parte de un atacante que tenga acceso físico a la máquina que quiera controlar (en casa, en la oficina, en una tienda...).

Técnicas usadas:

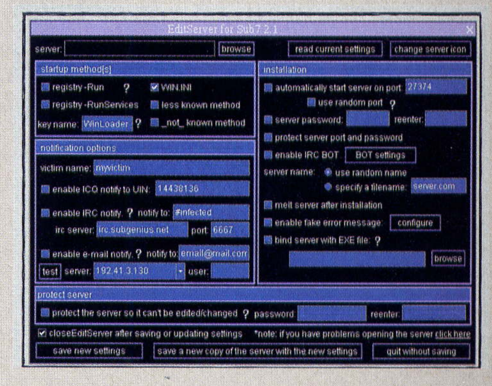
El programa servidor se instala en el directorio Windows con el nombre del programa que ha vehiculado la infección o usando otros nombres. Luego modifica el registro de Windows asociando el programa del servidor a todos los archivos con extensión .exe. De esta manera, se asegura el estar siempre en ejecución (cada vez que se lanza un programa, Subseven se activa). Si el servidor se mueve, no se podrá activar ningún programa (algunas versiones no dan este problema).
Cuando está en ejecución es completamente invisible en la lista de tareas, y si encuentra una conexión con Internet abierta, permanece a la espera de comandos por parte del cliente remoto.

Signos particulares:

Subseven puede individuarse de esta forma:
- Inserta nuevos valores en las claves de registro:
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunServices
- Inserta una nueva línea en la sección [windows] del archivo Win.ini [windows]
load=
run=c:\windows\server name .exe
Inserta una nueva línea en la sección [boot] de system.ini [boot]
...
shell=Explorer.exe c:\windows\server name
- Activa algún puerto TCP, normalmente el 27374, pero el puerto puede ser cambiado por el atacante.

Instrucciones para su parada:

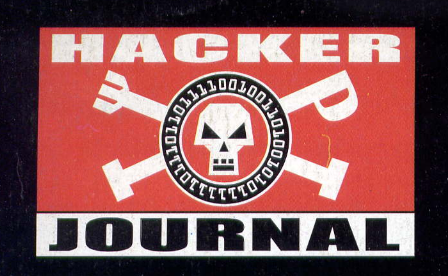
Incluso un buen antivirus perfectamente actualizado a veces no es capaz de contrastar un caballo de Troya. El atacante podría alterar la funcionalidad del antivirus, dejando al usuario una falsa sensación de seguridad.

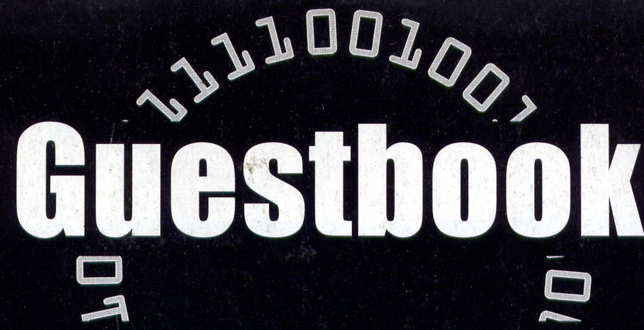


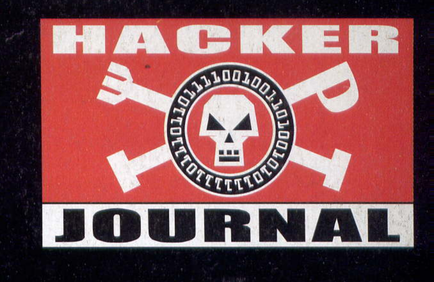
El modo más seguro para contrastarlo es consultar el sitio www.hackfix.org/subseven para determinar el número de versión del servidor e individuar el programa más adecuado para borrarlo.

Más información::

www.europe.f-secure.com/v-descs/subseven.shtml
www.symantec.com/avcenter/venc/data/backdoor.subseven.html

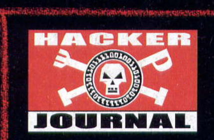






Las últimas firmas registradas en nuestro libro de visitas

A esta web "caí" por accidente inmediatamismo me di cuenta donde estaba,no la pensé 2 veces y me registré.Felicidades y adelante este 2004 q`hay mucho por hacer (.....perdón,por hackear....). Me interesa saber de qué manera adquirir todos los números de la revista "HJ", ¿o hay en versión ezine?. (ediez) • soy nuevo en el mundo de los hacker y me a gustao mucho esta revista y esta pagina asi que me gustaria que esta web siguiera creciendo. ¡¡¡¡ES LA MEJOR REVISTA QUE E VISTO EN MI VIDA!!!!!!!!!! (Juan Carlos) • Pinta buena la revista!! Soy de Argentina y me gustaria saber como puedo conseguir la revista, o que me la envien directamente.- Los Felicito por la revista y muchos EXITOS (porque suerte tiene cualquiera) happy hacking!!!! (Jorge) • Hola, queria saber como puedo conseguir los numeros 1,2 y 3 de vuestra revista, ya que me he comprado el numero 4 y me gusta mucho, espero que me los podais mandar, un saludo (Mary) • unSALUDparaLArevistaMAScañeraYqueríaCOMENTAROSsiPODEISenseñarCOMOrippeardiscosPARAhacerCOPIASdeSEGURIDADgraciasYarribaHACKERJOURNALfirmado(iniciadoENhackeo).....SX(XP (SX) • He visto en el quiosco una revista llamada Hackers Magazine al precio de 4.99 que incluye CD y según he comprobado son el mismo perro con distinto collar. ¿A quién va dirigida una y otra? Que se pretende con poner dos revistas? Que compremos las dos? Pues vais listos. La verdad, no entiendo muy bien la razón de poner dos revistas. Si quereis que el lector pueda tener una revista con CD pues añadirlo a Hacker Journal y no hagais experimentos. Esos... con gaseosa. (tron) • HEY HERMANOS SU MAGAZINE ES EL MEJOR, AHORA HA LLEGADO A MEXICO PERO SOLO EL #1, NO DEJEN DE MANDARLA! ESO DE KE NO LLEVA PUBLICIDAD ES DE LO MEJOR!!! SPERO Y SIGAN MANDANDO NUEVO MATERIAL AL NUEVO CONTINENTE. DESDE SALTILLO A l) 1 l (ADIKT0) • hola amigos les comento que en enero salio ala venta el numero 1 de su revista en mexico y los quiero felicitar , y comentarles que esta muy interesante espero que continue llegandonos en los kioskos dicen que asi sera bueno eso espero tambien me gustaria que iniciaran un curso para newbies que esten bien hasta luego (kross) • Hola hackers!! Ay una cuestion que me pongo en duda. Mi pregunta es como puedo passar de DIVX a DVD. En todos lo sitios sale como passar de DVD a DIVX!!! Pero como hacerlo al inverso!!! si alguiens es tan amable de contestarme el e-amil!! bye jouranleros!!! (cheddar bob) • Esta muy bien esta revista curraroslа mejor cada mes 8] (Alex) • Gracias por crear esta fabulosa revista (Zion) • Hola amigos ante todo me quito el sombrero ante vuestra revista es la caña. Hay q irse pensando una forma de q nos podamos subcribir o de ir incluyendo algún CD con programillas utiles y todo eso. Pero de momento la revista mola. Felicidades por vuestro trabajo. Saludos a los lectores de Hacker-Journal. (IronGolem)



Nos vemos en el próximo número

¡Resistid sin nosotros!

www.hacker-journal.com